US-CERT Cyber Security Bulletin

SB04-091 *March 31, 2004*

Information previously published in CyberNotes will now be incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 6 and March 30, 2004. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alt-N Technol-ogies [1] ***Exploit script published [2]***	Windows	**MDaemon/World Client 6.52 - 6.85**	**A buffer overflow vulnerability exists in the 'Form2Raw' component, which could let a remote malicious user execute arbitrary code.**	**Temporary Workaround:** **The vendor reports that you can disable the vulnerable Form2Raw code as follows: open the \MDaemon\WorldClient\WorldClient.ini file with Notepad and delete the following two lines:** **CgiBase2=/Form2Raw.cgi** **CgiFile2=C:\MDaemon\CGI\Form2Raw.exe** **Afterward, restart WorldClient to register the change.**	**MDaemon/ WorldClient 'Form2Raw' Remote Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**

[1] Hat-Squad Security Team Advisory, December 29, 2003.
[2] SecurityFocus, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[3] ***Vendors issue advisories* [4, 5]**	**Mac OS X 10.x, Unix**	**Apache 2.0.35-2.0.48**	**A remote Denial of Service vulnerability exists due to a handling error within the SSL engine when receiving normal HTTP requests on the SSL port of a SSL-enabled server.**	**Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.117&r2=1.118** ***Netwosix:* http://www.netwosix.org/adv06.html** ***Trustix:* http://www.trustix.org/errata/misc/2004/TSL-2004-0017-apache.asc.txt**	**Apache Mod_SSL HTTP Request Remote Denial of Service** **CVE Name: CAN-2004-0113**	**Low**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Apache Software Foundation[6]	MacOS X 10.x, Unix	Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48	An input validation vulnerability exists because escape character sequences can be injected into apache log files, which could let a remote malicious user create arbitrary files or execute arbitrary code.	Upgrades available at: http://httpd.apache.org/download.cgi **Netwosix** http://download.netwosix.org/0006/nepote	Apache Error Log Escape Sequence Injection CVE Name: CAN-2003-0020	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation[7]	MacOS X 10.x, Unix	Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.49	A vulnerability exists in 'mod_disk_cache' because sensitive information is stored in plaintext format, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Apache mod_disk_cache Module Client Authentication Credential Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation[8, 9]	MacOS X 10.x, Unix	Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48	A remote Denial of Service vulnerability exists via a listening socket on a rarely accessed port.	Upgrades available at: http://httpd.apache.org/download.cgi **Netwosix** http://download.netwosix.org/0006/nepote	Apache Connection Blocking Denial of Service CVE Name: CAN-2004-0174	Low	Bug discussed in newsgroups and websites.

[3] Secunia Advisory, SA11092, March 10, 2004.
[4] Netwosix Linux Security Advisory, LNSA-#2004-0006, March 25, 2004.
[5] Trustix Secure Linux Security Advisory, TSLSA-2004-0017, March 30, 2004.
[6] SecurityFocus, March 20, 2004.
[7] SecurityFocus, March 20, 2004.
[8] SecurityFocus, March 19, 2004.
[9] VU#132110, https://www.kb.cert.org/vuls/id/132110.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[10]	Windows NT 4.0/2000, MacOS X 10.x, Unix	Apache 1.0, 1.0.2, 1.0.3, 1.0.5, 1.1, 1.1.1, 1.2, 1.2.5, 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.7 – dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48	A vulnerability exists if the requested resource is served by an Apache module and not by the Apache Server itself, which could let a remote malicious user bypass LIMIT restrictions.	No workaround or patch available at time of publishing.	Apache HTAccess LIMIT Directive Bypass Configuration Error Weakness	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[11]	MacOS X 10.x	Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.2	A buffer overflow vulnerability exists when a remote malicious user connects to the admin service on TCP port 660 and submits 2057 characters, which could cause a Denial of Service and possibly allow the execution of arbitrary code.	No workaround or patch available at time of publishing.	Mac OS X Server Administration Service Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Atari [12]	Windows	Clever's Games Terminator 3: War of the Machines 1.0	A buffer overflow vulnerability exists in the 'ServerInfo' variable, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Clever's Games Terminator 3: War of the Machines Remote Client Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Belchior Foundry[13]	Windows, Unix	vCard 2.8	A vulnerability exists because the 'admin/uninstall.php' script does not authenticate remote users, which could let a remote malicious user bypass authentication.	No workaround or patch available at time of publishing.	VCard Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[10] SecurityFocus, March 14, 2004.
[11] Bugtraq, March 18, 2004.
[12] Securiteam, March 23, 2004.
[13] Bugtraq, March 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Borland/ Inprise[14]	Windows NT 4.0/2000, Unix	Interbase 4.0, 5.0, 6.0, 6.4, 6.5, 7.0, 7.1	A vulnerability exists in the 'admin.ib' user database file due to insecure default file permissions, which could let a malicious user obtain database administrative privileges.	No workaround or patch available at time of publishing.	Borland Interbase Unsafe Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Centrinity [15]	Windows NT 4.0/2000, MacOS, MacOS X	FirstClass 5.50, 5.77, 7.0, 7.1	A Cross-Site Scripting vulnerability exists in the 'Upload.shtml' script due to insufficient verification of the 'TargetName' parameter, which could let a remote malicious user execute arbitrary HTML or script code. *Note: The vendor has reported that this vulnerability only affects the 'standard' template set. The 'webmail' and 'mobile' template sets do not contain the 'Upload.shtml' script.*	No workaround or patch available at time of publishing.	FirstClass 'Upload.shtml' Script Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Check Point Software[16]	Multiple	Smart Dash-board	A buffer overflow vulnerability exists when the SmartTracker utility is used to add a firewall filter for Firewall-1, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Firewall-1 SmartDash-board Filter Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
clamav. Source forge.net [17]	Unix	ClamAV 0.65, 0.67	A remote Denial of Service vulnerability exists when a RAR archive that is created by variants of the W32.Beagle.A@mm worm is encountered.	Upgrades available at: http://prdownloads.sourceforge.net/clamav/clamav-0.68.tar.gz?download	ClamAV RAR Archive Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
CPanel, Inc.[18]	Unix	cPanel 9.1	Cross-Site Scripting vulnerabilities exist in the 'dodelautores.html' and 'addhandle.html' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	CPanel Multiple Remote Cross-Site Scripting Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[14] iDEFENSE Security Advisory, March 19, 2004.
[15] Secunia Advisory, SA11191, March 23, 2004.
[16] SecurityFocus, March 25, 2004.
[17] SecurityTracker Alert, 1009502, March 20, 2004.
[18] SecurityTracker Alert, 1009541, March 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Dame Ware Develop-ment LLC[19]	Windows NT 4.0/2000, XP	Mini Remote Control Server 3.70 .0.0-3.73 .0.0, 4.0	Several vulnerabilities exist: a vulnerability exists because the Blowfish encryption key is transmitted in plaintext when transferring files, which could let a remote malicious user obtain sensitive information; and a vulnerability exists due to a week random bit generator, which could let a remote malicious user enumerate or predict the encryption key.	No workaround or patch available at time of publishing.	Mini Remote Control Server Weak Encryption Implementa-tion & Weak Random Key Generation	Medium	Bug discussed in newsgroups and websites.
Dame Ware Develop-ment LLC[20]	Windows NT 4.0/2000, XP	Mini Remote Control Server 4.1.0.0	A vulnerability exists due to a weak random bit generator used to generate encryption keys, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Mini Remote Control Server Weak Random Key Generation	Medium	Bug discussed in newsgroups and websites.
Dame Ware Develop-men LLC[21]	Windows NT 4.0/2000, XP	Mini Remote Control Server 4.1.0.0	A vulnerability exists because the encryption key is sent over the network in plain text format, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	DameWare Mini Remote Control Server Clear Text Encryption Key Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
emil[22]	Unix	emil 2.0.4, 2.0.5, 2.1.0-beta9	Multiple vulnerabilities exist: a buffer overflow vulnerability exists due to boundary errors exist within the 'encode_mime(),' 'encode_uuencode(),' and 'decode_uuencode()' functions, which could let a local/remote malicious user execute arbitrary code; and format string errors exist in various functions when constructing error messages, which could let a local/remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/e/emil/	Emil Multiple Buffer Overflow & Format String	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
eSignal[23]	Windows	eSignal 7.5, 7.6	A buffer overflow vulnerability exists due to a due to a boundary error within 'Specs.dll' when parsing incoming data requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	ESignal Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[19] Secunia Advisory, SA11205, March 24, 2004.
[20] Securiteam, March 25, 2004.
[21] SecurityFocus, March 23, 2004.
[22] Debian Security Advisory, DSA 468-1, March 24, 2004.
[23] Secunia Advisory, SA11222, March 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group[24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36]	Windows 95/98/ME/ NT 4.0, Unix	Ethereal 0.8.13, 0.8.14, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.2	Multiple vulnerabilities exist: Thirteen stack-based buffer overflow vulnerabilities exist in various protocol dissectors (BGP, EIGRP, IGAP, IRDA, NetFlow, PGM, UCP, NetFlow, IrDA, ISUP, and TCAP), which could let a remote malicious user execute arbitrary code; a remote Denial of Service exists when a malicious user submits a carefully-crafted RADIUS packet; a remote Denial of Service vulnerability exits due to a zero length Presentation protocol selector; and a remote Denial of Service vulnerability exist within the handling of malformed color filter files.	Upgrades available at: http://www.ethereal.com/download.html	Ethereal Multiple Vulnerabilities CVE Names: CAN-2004-0176, CAN-2004-0365, CAN-2004-0367	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Expinion. net[37]	Windows NT 4.0/2000, XP, 2003	Member Manage-ment System 2.1	A vulnerability exists in the 'resend.asp' and 'news_view.asp' scripts due to insufficient validation of user-supplied input in the 'ID' parameter, which could let a remote malicious user execute arbitrary SQL code.	No workaround or patch available at time of publishing.	Member Management System ID Parameter SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Expinion. net[38]	Windows NT 4.0/2000, XP, 2003	Member Manage-ment System 2.1	A Cross-Site Scripting vulnerability exists in the 'error.asp' and 'register.asp' scripts due to insufficient sanitization of the 'err' parameter, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Member Management System Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[24] Ethereal Advisory, enpa-sa-00013, March 22, 2004.
[25] VU#119876, https://www.kb.cert.org/vuls/id/119876.
[26] VU#124454, https://www.kb.cert.org/vuls/id/124454.
[27] VU#125156, https://www.kb.cert.org/vuls/id/125156.
[28] VU#433596, https://www.kb.cert.org/vuls/id/433596.
[29] VU#591820, https://www.kb.cert.org/vuls/id/591820.
[30] VU#644886, https://www.kb.cert.org/vuls/id/644886.
[31] VU#659140, https://www.kb.cert.org/vuls/id/659140.
[32] VU#695486, https://www.kb.cert.org/vuls/id/695486.
[33] VU#740188, https://www.kb.cert.org/vuls/id/740188.
[34] VU#792286, https://www.kb.cert.org/vuls/id/792286.
[35] VU#864884, https://www.kb.cert.org/vuls/id/864884.
[36] VU#931588, https://www.kb.cert.org/vuls/id/931588.
[37] SecurityFocus, March 20, 2004.
[38] SecurityFocus, March 20, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Expinion.net[39]	Windows NT 4.0/2000, XP, 2003	News Manager Lite 2.5	Vulnerabilities exist in the 'comment_add.asp,' 'search.asp,' 'category_news_headline.asp,' 'more.asp,' 'category_news.asp,' and 'ews_sort.asp' scripts, which could let a remote malicious user execute arbitrary code or obtain administrative access.	No workaround or patch available at time of publishing.	Expinion.net News Manager Lite Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
fizmez.com [40]	Windows, Unix	Fizmez Web Server 1.0	A Denial of Service vulnerability exists in the connection handler due to a NULL pointer dereference error.	Upgrade available at: http://fizmez.com/downloads/fws-1.1.tar.gz	Fizmez Web Server Null Connection Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a telnet client.
Florian Heinz[41]	Unix	Nstx IP Over DNS Utility 1.0, 1.1, beta1-beta3	A remote Denial of Service vulnerability exists when a malicious user submits specially crafted input to the target system on UDP port 53.	Upgrades available at: http://nstx.dereference.de/nstx/nstx-1.1-beta4.tgz	NSTX Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Fluid Games[42]	Windows	The Rage 1.0 1	A remote Denial of Service vulnerability exists when processing client request packets containing 0 for the values of the client IP address and port number.	No workaround or patch available at time of publishing.	The Rage Game Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit scripts have has been published.
Foxmail[43]	Windows	Foxmail Email Client - Chinese Version 4.2, 5.0, English Version 4.1	A buffer overflow vulnerability exists due to a failure to verify buffer boundaries when processing user supplied e-mail headers, which could let a remote malicious user cause a Denial of Service and execute arbitrary code.	No workaround or patch available at time of publishing.	Foxmail Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Francisco Burzi[44]	Windows, Unix	PHP-Nuke 7.1	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied data via the 'Your Name,' 'nicname,' 'fname,' 'ratenum,' and 'search' fields of 'modules.php' script, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHP-Nuke Modules.php Multiple Cross-Site Scripting Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however a Proof of Concept exploit has been published.

[39] SecurityFocus, March 20, 2004.
[40] Secunia Advisory, SA11141, March 17, 2004.
[41] Rstack Team (Rstack.org) Security Advisory, March 25, 2004.
[42] Bugtraq, March 23, 2004.
[43] SecurityFocus, March 23, 2004.
[44] waraxe-2004-SA#005, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[45]	Widows, Unix	PHP-Nuke 6.0, 6.5, RC1-RC3, 6.5 FINAL, 6.5 BETA1, 6.6, 6.7, 6.9, 7.0, 7.0 FINAL, 7.1	A vulnerability exists due to a design error when arbitrary URI values are specified in bbCode tags, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP-Nuke Image Tag Admin Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
FVWM[46]	Multiple	FVWM 2.4.17, 2.5.8	A vulnerability exists in the 'fvwm_make_browse_menu. sh' script, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	FVWM fvwm_make_ browse_menu. sh Scripts Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
FVWM[47]	Multiple	FVWM 2.4.17, 2.5.8	A vulnerability exists in the 'fvwm_make_directory_menu. sh' script, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	fvwm_make_ directory_ menu.sh Scripts Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Global SCAPE, Inc. [48]	Windows	Global SCAPE Secure FTP Server 2.0 Build 03.11.2004.2	A buffer overflow vulnerability exists due to an out-of-bounds write error within the handling of arguments passed to 'SITE' commands, which could let a remote malicious user execute arbitrary code.	Update available at: www.cuteftp.com/gsftps/	GlobalSCAPE Secure FTP Server SITE Command Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
GNOME [49]	Unix	Gnome 2.0-2.4	A vulnerability exists due to a problem in gnome-session during initialization of the 'LD_LIBRARY_PATH' environment variable when starting GNOME via '/usr/X11R6/bin/gnome,' which could let a malicious user obtain elevated privileges.	**Conectiva:** ftp://ul.conectiva.com.br/updates/1.0/RPMS.core/gnome-session-2.0.5-222.i586.rpm	Gnome 'LD_ LIBRARY_ PATH' Elevated Privileges	Medium	Bug discussed in newsgroups and websites.
GNU[50]	Multiple	SPIP 1.7	A vulnerability exists because user input passed to certain parameters in the 'forum.php 3' script isn't properly sanitized, which could let a remote malicious user execute arbitrary PHP code.	Patches available at: http://www.e-glop.net/dev/spip/	GNU SPIP 'forum.php3"' PHP Code Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[45] SecurityFocus, March 16, 2004.
[46] SecurityFocus, March 19, 2004.
[47] SecurityFocus, March 19, 2004.
[48] Securiteam, March 17, 2004.
[49] Conectiva Security Advisory, CLSA-2004:823, March 26, 2004.
[50] Secunia Advisory, SA11127, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [51]	Windows	Web Jetadmin 7.5.2456	Multiple vulnerabilities exist: a vulnerability exists because it is possible to upload HTS files using '/plugins/hpjwja/script/devices_update_printer_fw_upload.hts,' which could let a remote malicious user execute arbitrary code; a vulnerability exists in '/plugins/hpjdwm/script/test/setinfo.hts' due to insufficient verification of the 'setinclude' parameter, which could let a remote malicious obtain sensitive information or execute arbitrary code; a vulnerability exists because a remote authenticated malicious user can upload a specially crafted script and execute the script to cause 'hpwebjetd' to crash; and a vulnerability exists because it is possible to inject arbitrary commands that will be executed when the service is restarted.	No workaround or patch available at time of publishing.	Jetadmin Printer Firmware Update Script Arbitrary File Upload Weakness	Low/ Medium/ **High** **(Low if a DoS; Medium is sensitive informa-tion can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser. There is no exploit required for the information disclosure vulnerability. Proof of Concept exploit has been published for the remote arbitrary code execution vulnerability.
Hibyte Ltd. [52]	Windows, Unix	HiGuest	A vulnerability exists in the message form field in the guestbook entry submission form, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	HiGuest Message Field HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM[53]	Unix	AIX 4.3.3	A buffer overflow vulnerability exists in GNU make for IBM AIX due to insufficient boundary checks when reading the path to the CC compiler, which could let a malicious user obtain ROOT privileges.	No workaround or patch available at time of publishing.	GNU Make For IBM AIX CC Path Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
IBM[54]	Unix	AIX 4.3.3	A buffer overflow vulnerability exists in the 'getlvcb' utility, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AIX 'Getlvcb' Utility Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[51] Bugtraq, March 24, 2004.
[52] SecurityFocus, March 23, 2004.
[53] SecurityFocus, March 17, 2004.
[54] SecurityFocus, March 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[55]	Unix	AIX 4.3.3	A buffer overflow vulnerability exists in the 'putlvcb' utility, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AIX 'Putlvcb' Utility Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
IBM[56]	Unix	AIX 4.3.3, 5.1 L, 5.1	A vulnerability exists in 'invscoutd' because a logfile may be specified as a command line argument, which could let a malicious user create or overwrite files with elevated privileges.	No workaround or patch available at time of publishing.	AIX 'invscoutd' Insecure Logfile Handling	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Internet Security Systems[57]	Windows	BlackICE PC Protection 3.6, ccg, ccf, cce, ccd, ccc, ccb, cca, cbz, cbr, cbd, cbz, BlackIce Server Protection 3.5 cdf, 3.6, ccg, Internet Security Systems BlackIce Server Protection 3.6 ccf, cce, ccd, ccc, ccb, cca, cbz, cbr	A vulnerability exists due to a misconfiguration in the default settings of BlackICE PC Protection, which could result in a decrease in the level of protection that the software provides.	Upgrades available at: http://blackice.iss.net/issEn/DLC/consumer/	BlackICE PC/Server Protection Weak Default Configuration	Medium	Bug discussed in newsgroups and websites.

[55] SecurityFocus, March 17, 2004.
[56] SecurityFocus, March 26, 2004.
[57] SecurityFocus, March 27, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Internet Security Systems[58, 59]	Windows NT 4.0/2000	Real Secure Network 7.0, XPU 22.11& prior, Server Sensor 7.0 XPU 22.11 & prior, 6.5 for Windows SR 3.10 & prior, Proventia A Series XPU 22.11 & prior, G Series XPU 22.11 & prior, M Series XPU 1.9 & prior, Real Secure Desktop 7.0 ebl & prior, 3.6 ecf & prior, Real Secure Guard 3.6 ecf & prior, Real Secure Sentry 3.6 ecf & prior, BlackICE Agent for Server 3.6 ecf & prior, BlackICE PC Protection 3.6 ccf & prior, BlackICE Server Protection 3.6 ccf & prior	A buffer overflow vulnerability exists due to a boundary error in the PAM (Protocol Analyses Module) component within a routine used for monitoring ICQ server responses, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.iss.net/download/	Internet Security Systems Protocol Analysis Module Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability is being actively exploited in the wild. The W32. Witty Worm exploits this issue and it is propagating with a fixed source port of UDP port 4000. The worm appears to be contained in a single UDP datagram.

[58] Bugtraq, March 18, 2004.

[59] VU#947254, https://www.kb.cert.org/vuls/id/947254.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Invision Power Services[60] ***Patches now available*** [61]	**Windows, Unix**	**Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2, 1.3, 2.0, 2.0 Alpha 3**	**An input validation vulnerability exists in 'search.php' due to insufficient sanitization of the 'st' parameter, which could let a remote malicious user execute arbitrary code.**	***Patches available at:*** **http://forums.invisionpower.com/index.php?s=bc4e9438d266206887560633dce21d30&act=Attach&type=post&id=1298**	**Invision Power Board Input Validation**	**High**	**Bug discussed in newsgroups and websites.**
Invision Power Services [62]	Windows, Unix	Invision Power Top Site List 1.0, 1.1 RC2 1.1	A vulnerability exists in 'index.php' due to insufficient validation of user-supplied input in the 'id' parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Invision Power Top Site List Input Validation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Invision Power Services [63]	Windows, Unix	Invision Gallery 1.0.1	Multiple SQL injection vulnerabilities exist in the 'index.php' script due to insufficient sanitization of user-supplied data via the 'img,' 'cat,' 'sort_key,' 'order_key,' 'user,' and 'album' parameters, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Invision Gallery Multiple Input Validation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
IP3 Networks [64]	Multiple	IP3 NetAccess - Campus & MDUs, Hospitality, Wireless HotSpots, Wireless HotZones & Small Hotels, Wireless ISPs & MDUs	A vulnerability exists due to a failure to properly sanitize user input, which could let a remote malicious user obtain full control of the appliance.	Update available at: http://www.ip3networks.com/	IP3 NetAccess Appliance SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[60] Secunia Advisory, SA11008, March 1, 2004.
[61] SecurityFocus, March 20, 2004.
[62] Bugtraq, March 22, 2004.
[63] Bugtraq, March 22, 2004.
[64] SecurityFocus, March 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IpSwitch[65]	Windows 95/98/NT 3.1/4.0/ 2000, XP	WS FTP Server 1.0.1-1.0.5, 2.0-2.0.4, 3.0, 3.01, 3.1-3.1.3, 3.4, 4.0-4.02, WS_FTP Pro 6.0, 7.5, 8.0 2, 8.0 3	Multiple vulnerabilities exist: a vulnerability exists in the 'SITE SETS' FTP command, which could let a local/remote malicious user execute arbitrary programs with SYSTEM privileges; a buffer overflow vulnerability exists within the ALLO handler when returning error strings to a client, which could let a remote malicious user execute arbitrary programs with SYSTEM privileges; a buffer overflow vulnerability exists within the handling of the 'STAT' FTP command while downloading files, which could let a remote malicious user execute arbitrary code with SYSTEM privileges; and a remote Denial of Service vulnerability exists when a malicious user submits an extremely large value as an argument to the 'REST' FTP command and then by uploading a small file with the "STOR" FTP command.	No workaround or patch available at time of publishing.	WS_FTP Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
IpSwitch[66]	Windows	WS_FTP Pro 8.0 3 WS_FTP Pro 8.0 2	A buffer overflow vulnerability exists due to a boundary error within the client when processing ASCII mode directory data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WS_FTP Pro Client Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
IpSwitch[67]	Windows	WS_FTP Pro 8.0 3	A buffer overflow vulnerability exists when the client views directory listings containing files and directory names of excessive length without a terminating CR/LF character, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WS_FTP Pro Client Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
itez Multi-media Solutions[68]	Windows	Picophone Internet Telephone 1.63	A buffer overflow vulnerability exists due to a failure to verify the size of user-supplied input, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.vitez.it/picophone/PicoPhone164.exe	PicoPhone Internet Phone Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[65] Bugtraq, March 23, 2004.
[66] Bugtraq, March 14, 2004.
[67] Bugtraq, March 16, 2004.
[68] Securiteam, March 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jelsoft Enterprises[69]	Windows, Unix	vBulletin 2.0, beta 2&3, 2.0.1, 2.0.2, 2.2.0-2.2.9 can, 2.3, 2.3.3, 2.3.4	Cross-Site Scripting vulnerabilities exist because the 'showthread.php,' 'forumdisplay.php,' and 'memberlist.php' files do not properly filter HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	VBulletin Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proofs of Concept exploits have been published.
Jelsoft Enterprises [70]	Windows, Unix	vBulletin 2.0, beta 2&3, 2.0.1-2.0.2, 2.2.0-2.2.9 can, 2.3, 2.3.3, 2.3.4	A Cross-Site Scripting vulnerability exists in the 'private.php' script due to a failure to sanitize user input, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	VBulletin 'Private.PHP' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Jelsoft Enterprises [71]	Windows, Unix	vBulletin 2.0, beta 2&3, 2.0.1-2.0.2, 2.2.0-2.2.9 can, 2.3, 2.3.3, 2.3.4, 3.0.0 can4, 3.0.0	A Cross-Site Scripting vulnerability exists in the 'index.php' script in both the 'admincp' and 'modcp' application directories due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	VBulletin Multiple Module Index.PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Jetty[72]	Unix	Jetty 4.1 .0RC4, 4.1 .0, 4.1.1, 4.2.4-4.2.7, 4.2.9, 4.2.11, 4.2.12, 4.2.14-4.2.18	An unspecified Denial of Service vulnerability exists in Jetty Java HTTP Servlet Server.	Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=7322	Jetty Unspecified Denial of Service	Low	Bug discussed in newsgroups and websites.
Joel Palmius[73]	Unix	Mod_ Survey 3.0 .0-3.0.16 pre1, 3.2 .0-pre1-pre3	A vulnerability exists in survey fields due to insufficient filtering of input, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: http://gathering.itm.mh.se/modsurvey/download/test/	Mod_Survey Survey Input Field HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[69] GulfTech Security Research Team Advisory, March 15, 2004.
[70] SecurityFocus, March 22, 2004.
[71] SecurityFocus, March 22, 2004.
[72] Secunia Advisory, SA11166, March 19, 2004.
[73] Mod_Survey Security Advisory, March 22, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Kerio Technol-ogies[74]	Windows	Mail server 5.7.0-5.7.6	A buffer overflow vulnerability exists in the spam filter component, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrades available at: http://www.kerio.com/kms_download.html	Kerio MailServer Spam Filter Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Kerio Technol-ogies [75]	Windows NT 4.0/2000, XP	WinRoute Firewall 5.0.1-5.0.9, 5.1-5.1.9	A Denial of Service vulnerability exists due to a flaw in the parsing of HTTP headers.	Upgrade available at: http://www.kerio.com/kwf_history.html	WinRoute Firewall Malformed HTTP Header Denial of Service	Low	Bug discussed in newsgroups and websites.
Lim Unlimited [76]	Unix	Crafty 19.3	A buffer overflow vulnerability exists due to insufficient bounds checking performed by 'crafty.bin,' which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Crafty 'crafty.bin' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mambo[77]	Windows, Unix	Mambo Open Source 4.5 (1.0.1), (1.0.0)	A Cross-Site Scripting vulnerability exists because user input passed to the 'return' and 'mos_change_template' parameters in 'index.php' and other scripts isn't properly sanitized, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Mambo Open Source Index.PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
MathoPD [78]	Unix	Mathopd Web Server 1.2, 1.3, 1.3 p4-p8, 1.3 p17, 1.3 p18, 1.4, 1.4p1, 1.5 b13	A buffer overflow vulnerability exists due to a failure to check the bounds of a buffer storing user-supplied input, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.mathopd.org/dist/	MathoPD Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[74] SecurityFocus, March 25, 2004.
[75] Secunia Advisory, SA11204, March 24, 2004.
[76] Bugtraq, March 15, 2004.
[77] GulfTech Security Research Team Advisory, March 15, 2004.
[78] Securiteam, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Maty Scripts[79]	Multiple	MS-Analysis Website Traffic Analyzer 2.0	Multiple vulnerabilities exist: a vulnerability exists because several scripts return error messages containing the full installation path if called directly, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists because input passed to various parameters in several scripts isn't properly verified before it is returned to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists because the 'referer' header isn't properly validated before it is inserted into the database, which could let a remote malicious user manipulate SQL queries or extract data.	No workaround or patch available at time of publishing.	MS-Analysis Module Multiple Remote Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proof of Concepts have been published.
Microsoft[80]	Windows XP	Windows XP Home, SP1, XP Media Center Edition, Professional, SP1	A remote Denial of Service vulnerability exists when a malicious directory that contains 'wmf' files is submitted to a vulnerable user via e-mail or other means.	No workaround or patch available at time of publishing.	Windows XP explorer.exe Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[81]	Windows XP	Windows XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A remote Denial of Service vulnerability exists in the 'shell:' command due to a failure to properly validate user-supplied input. including a URI in an HTML tag.	No workaround or patch available at time of publishing.	Windows XP Explorer.EXE Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Microsoft[82]	Windows NT 4.0/2000	Windows Media Services, 4.0, 4.1	A buffer overflow vulnerability exists due to a problem with how the logging ISAPI extension handles incoming client MX_STATS_LogLine: header field data in POST requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Media Services MX_STATS_\ LogLine NSIISlog.DLL Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[79] waraxe-2004-SA#011, March 22, 2004.
[80] SecurityFocus, March 16, 2004.
[81] Bugtraq March 19, 2004.
[82] SecurityFocus, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [83]	Windows NT 4.0	Visual C++ 6.0, SP1-SP5, Visual Studio 6.0, SP1-SP5	A Denial of Service vulnerability exists because the MFC (Microsoft Foundation Classes) ISAPI (Internet Server Application Programming Interface) code may produce invalid arguments when processing data from POST requests.	This issue will reportedly be addressed with the release of Microsoft Visual Studio 6 Service Pack 6, which will be listed at the following page when it is released: http://msdn.microsoft.com/vstudio/downloads/updates/sp/	Visual C++ Constructed ISAPI Extensions Denial of Service	Low	Bug discussed in newsgroups and websites.
Modsecurity.org [84, 85]	Unix	mod_ mod_security security 1.7.4	An off-by-one buffer overflow vulnerability exists when the 'SecFilterScanPost' directive is enabled, which could let a remote malicious user execute arbitrary code..	Upgrade available at: http://www.modsecurity.org/download/mod_security-1.7.5.tar.gz	Apache Mod_Security Module SecFilterScanPost Off-By-One Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Mozilla.org [86] ***RedHat issues advisory***[87]	**Windows 95/98/ME/ NT 4.0/2000, MacOS, MacOS X, Unix**	**Mozilla Browser 0.8, 0.9.2.1, 0.9.2-0.9.9, 0.9.35, 0.9.48, 1.0, RC1& RC2, 1.0.1, 1.0.2, 1.1-1.5**	**A Cross-Site Scripting vulnerability exists in 'nsDOMClassInfo.cpp' and occurs when a large number of event handlers are used within HTML tags, which could let a remote malicious user execute arbitrary code.**	**The vulnerability has been fixed in versions 1.6b and 1.4.2 available at:** **http://www.mozilla.org/** ***RedHat:*** **ftp://updates.redhat.com/9/en/os/**	**Mozilla Browser Zombie Document Cross-Site Scripting** **CVE Name: CAN-2004-0191**	**High**	**Bug discussed in newsgroups and websites.**
Multiple Vendors [88]	MacOS X 10.x, Unix	OpenSSH OpenSSH 3.0, p1, 3.0.1, p1, 3.0.2, p1, 3.1, p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3, p1, 3.4, p1	A vulnerability exists in the OpenSSH ‘scp’ utility, which could let a malicious user corrupt files.	**Conectiva:** ftp://ul.conectiva.com.br/updates/1.0/RPMS.core/openssh-3.4p1-263.i586.rpm	OpenSSH ‘SCP’ Client File Corruption	Medium	Bug discussed in newsgroups and websites.

[83] Secunia Advisory, SA11199, March 24, 2004.
[84] S-Quadra Advisory #2004-03-15, March 15, 2004.
[85] VU#779438, https://www.kb.cert.org/vuls/id/779438.
[86] Public Security Advisory, Sandblad #13, February 25, 2004.
[87] Red Hat Security Advisory, RHSA-2004:112-01, March 18, 2004.
[88] Conectiva Security Advisory, CLSA-2004:831, March 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[89]	Multiple	Francisco Burzi PHP-Nuke 6.0, 6.5, BETA 1, FINAL, RC1-RC3, 6.6, 6.7, 6.9, 7.0, FINAL, 7.1; phpBB Group phpBB 2.0 .0, Beta 1, RC1-RC4, 2.0.1-2.0.8	A vulnerability exists in the 'privmsg.php' phpBB script due to insufficient sanitization, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBB 'privmsg.php' Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concept exploits have been published.
Multiple Vendors[90]	Unix	Linux kernel 2.4, 2.4.0-test1- test 12, 2.4.1-2.4.21	Multiple vulnerabilities exist, which could let a malicious user obtain sensitive information via the 'ext3' filesystem, cause a Denial of Service via the SoundBlaster code, cause a Denial of Service via Kernel DRI support and cause a Denial of Service via 'mremap.'	**Conectiva:** http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000829	Multiple Local Linux Kernel Vulnerabilities	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites.
Multiple Vendors [91, 92] ***Trustix issues advisory***[93]	**Unix**	**RedHat sysstat-4.0.7-3.i386. rpm; SGI ProPack 2.3, 2.4; Sysstat Sysstat 4.0.7, 4.1.1-4.1.7, 5.0.1**	**Two vulnerabilities exist: a vulnerability exists in the monitoring utility due to insecure creation of temporary files, which could let a malicious user corrupt system files, cause a loss of data, or a Denial of Service; and a vulnerability exists in the 'isag' utility because temporary files are created with predictable names, which could let a malicious user cause a Denial of Service or obtain elevated privileges.**	**RedHat:** **ftp://updates.redhat.com/9/en/os/i386/sysstat-4.0.7-4.rhl9.1.i386.rpm** **SGI:** **ftp://patches.sgi.com/support/free/security/patches/ProPack/** **Sysstat:** **http://perso.wanadoo.fr/sebastien.godard/download_en.html** ***Trustix:*** **http://www.trustix.org/errata/misc/2004/TSL-2004-0011-sysstat.asc.txt**	**Sysstat Insecure Temporary File Creation & Names** **CVE Names: CAN-2004-0107, CAN-2004-0108**	**Low/ Medium** **(Medium if data is corrupted or lost)**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[89] waraxe-2004-SA#013, March 26, 2004.
[90] Conectiva Security Advisory, CLSA-2004:829, March 26, 2004.
[91] Red Hat Security Advisory, RHSA-2004:093-01, March 10, 2004.
[92] SGI Security Advisory, 20040302-01-U, March 12, 2004.
[93] Trustix Secure Linux Security Advisory, TSLSA-2004-0011, March 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113]	Unix	OpenSSL 0.9.6c - 0.9.6k, 0.9.7a - 0.9.7c	Multiple remote Denial of Service vulnerabilities exist: a vulnerability exists when a remote malicious user performs a specially crafted SSL/TLS handshake due to a null-pointer assignment in the 'do_change_cipher_spec()' function; a vulnerability exists due to a flaw in a patch introduced in 0.9.6d; and a vulnerability exists because there is a flaw when performing SSL/TLS handshakes using Kerberos cipher suites.	**4D WebSTAR:** ftp://ftp.4d.com/products/webstar/current/4d_webstar_v/4d_webstar_v.sit **BlueCoat:** http://www.bluecoat.com/support/knowledge/advisory_openSSL_can-2004-0079.html **Cisco:** http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml#software **Debian:** http://security.debian.org/pool/updates/main/o/openssl/ **Engarde:** http://infocenter.guardiandigital.com/advisories/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:05/openssl.patch **Lite Speed:** http://www.litespeedtech.com/download.html **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **Netwosix:** http://download.netwosix.org/0005/nepote **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.3/c **OpenPKG:** ftp.openpkg.org **OpenSSL:** ftp://ftp.openssl.org/source/ **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-119.html **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Sun:** http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57524 **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ **Tarantella:** http://www.tarantella.com/security/bulletin-10.html **Trustix:** http://http.trustix.org/pub/trustix/updates/	OpenSSL Denial of Service Vulnerabilities CVE Names: CAN-2004-0079, CAN-2004-0081, CAN-2004-0112	Low	Bug discussed in newsgroups and websites.

[94] Debian Security Advisory, DSA 465-1, March 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [114, 115]	Windows NT 4.0/2000, XP, Unix	Macromedia Cold Fusion MX 6.0, 6.1, J2EE 6.0, J2EE 6.1, JRun 4.0, SP1a & SP1, 4.0 build 61650; Sun ONE Application Server 7.0 UR2 Upgrade Standard, Upgrade Platform, Standard Edition, Platform Edition, 7.0 UR1 Standard Edition, Platform Edition, 7.0 Standard Edition, Platform Edition	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted SOAP request.	**Macromedia:** http://www.macromedia.com/devnet/security/security_zone/mpsb04-04.html **Sun:** http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57517	Multiple Vendor SOAP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[95] Guardian Digital Security Advisory, ESA-20040317-003, March 17, 2004.
[96] FreeBSD Security Advisory, FreeBSD-SA-04:05, March 17, 2004.
[97] Netwosix Linux Security Advisory, LNSA-2004-0005, March 17, 2004.
[98] Mandrakelinux Security Update Advisory, MDKSA-2004:023, March 17, 2004.
[99] Red Hat Security Advisory, RHSA-2004:121-01, March 17, 2004.
[100] NetScreen Advisory, 58466, M arch 17, 2004.
[101] SUSE Security Announcement, SuSE-SA:2004:007, March 17, 2004.
[102] Trustix Secure Linux Security Advisory, TSLSA-2004-0012, March 18, 2004.
[103] Slackware Security Advisory, SSA:2004-077-01, March 18, 2004.
[104] Stonesoft Corp. Security Advisory, March 19, 2004.
[105] Tarantella Security Bulletin #10, March 19, 2004.
[106] OpenPKG Security Advisory, OpenPKG-SA-2004.007, March 18, 2004.
[107] Fedora Update Notification, FEDORA-2004-095, March 19, 2004.
[108] BlueCoat Security Advisory, March 22,2004.
[109] Cisco Security Advisory, 49898 Rev 1.3, March 23, 2004.
[110] Sun(sm) Alert Notification, 57524, March 23, 2004.
[111] VU#288574, https://www.kb.cert.org/vuls/id/288574.
[112] VU#465542, https://www.kb.cert.org/vuls/id/465542.
[113] VU#484726, https://www.kb.cert.org/vuls/id/484726.
[114] Macromedia Security Bulletin, MPSB04-04, March 15, 2004.
[115] Sun(sm) Alert Notification, 57517, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [116, 117]	Unix	Open Group CDE Common Desktop Environment 1.0.1, 1.0.2, 1.1, 1.2, 2.0, 2.1 20, 2.1; Xi Graphics DeXtop 2.1, 3.0	A vulnerability exists due to a double-free error in 'dtlogin' when parsing XDMCP (X Display Manager Control Protocol) requests, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Common Desktop Environment DTLogin XDMCP Parsing	**High**	Bug discussed in newsgroups and websites.
MySQL AB[118]	Unix	MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0.0-4.0.15, 4.1.0-alpha, 4.1.0-0	A vulnerability exists in the reporting utility (mysqlbug) because temporary files are created with a static name when a bug report is aborted, which could let a malicious user corrupt files, destroy dat a and cause a Denial of Service.	Update available at: http://www.mysql.com/doc/en/Installing_source_tree.html	MySQL 'mysqlbug' Temporary File	Low/ Medium (Medium if data is destroyed or corrupted)	Bug discussed in newsgroups and websites. There is no exploit code required.
Mythic Entertainment [119]	Windows	Dark Age of Camelot 1.60-1.68	An encryption key signing vulnerability exists due to a design error in the application that carries out encryption without having the encryption key signed or verified by the affected server, which could let a malicious user carry out man-in-the-middle attacks against a vulnerable system or obtain sensitive information.	No workaround or patch available at time of publishing.	Mythic Entertainment Dark Age of Camelot Encryption Key Signing	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[116] Secunia Advisory, SA11210, March 25, 2004.
[117] VU#179804, https://www.kb.cert.org/vuls/id/179804.
[118] Bugtraq, March 24, 2004.
[119] Securiteam, March 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nexgen server. com [120]	Windows NT 4.0/2000, XP	Nexgen FTP Server 1.0	A Directory T raversal vulnerability exists due to insufficient verification, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NexGen FTP Server Remote Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Nival Interactive [121]	Windows	Etherlords 1.0 1-1.07, 1.0, Nival Etherlords II 1.01-1.0 3, 1.0	A remote Denial of Service vulnerability exists due to a failure to properly validate user-supplied network data.	No workaround or patch available at time of publishing.	Etherlords Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Novell[122]	Multiple	Netware 6.5 SP1.1(a)	A vulnerability exists because admin/install passwords are stored in the 'NIOUTPUT.TXT' and 'NT.LOG' installation log files, which could let a malicious user obtain sensitive information.	Update information available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2968534.htm	NetWare Admin/Install Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell[123]	Multiple	Group wise 6.0, SP1-SP4, 6.5, SP1& SP2	A configuration vulnerability exists in the 'GWAPACHE.CONF' file when running with Apache Web Server for NetWare, which could let a remote malicious user obtain unauthorized access.	Fix available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10091330.htm	Novell GroupWise WebAccess Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NullSoft [124]	Windows 95/98/ME/ NT 3.5.1, 4.0/2000, XP	Winamp 2.4, 2.5 E, 2.5 e, 2.64, 2.10, 2.24, 2.50, 2.60 (lite), (full), 2.61 (full), 2.62 (standard) 2.64 (standard) 2.65, 2.70, (full), 2.71-2.81, 2.91, 3.0, 3.1, 5.0 1	A Denial of Service vulnerability exists when processing malformed file names.	No workaround or patch available at time of publishing.	Winamp Malformed File Name Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[120] Securiteam, March 25, 2004.
[121] Securiteam, March 30, 2004.
[122] Novell Technical Information Document, TID2968534, March 20, 2004.
[123] Novell Technical Information Document, TID10091330, March 8, 2004.
[124] SecurityTracker Alert, 1009499, March 19, 2004,

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
oftpd[125]	Unix	oftpd 0.3.0-0.3.6	A remote Denial of Service vulnerability exists due to an handling error when a PORT command is received.	Upgrades available at: http://www.time-travellers.org/oftpd/oftpd-0.3.7.tar.gz	OFTPD Port Argument Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenBSD[126]	Unix	OpenBSD 3.3, 3.4	A vulnerability exists in the httpd access module due to an error in the parsing of Allow/Deny rules with IP addresses without a netmask, which could let a remote malicious user obtain unauthorized access.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/	OpenBSD httpd Access Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenBSD[127]	Unix	OpenBSD –current, 3.3, 3.4	Multiple remote Denial of Service vulnerabilities exist when processing certain malformed payloads.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/	OpenBSD isakmpd Multiple Unspecified Remote Denial of Service CVE Names: CAN-2004-0218, CAN-2004-0219, CAN-2004-0220, CAN-2004-0221, CAN-2004-0222	Low	Bug discussed in newsgroups and websites.
Opera Software[128]	Windows, unix	Opera Web Browser 7.22, 7.23	A remote Denial of Service vulnerability exists when handling large JavaScript arrays.	No workaround or patch available at time of publishing.	Opera Web Browser Large JavaScript Array Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[125] SecurityFocus, March 26, 2004.
[126] SecurityFocus, March 14, 2004.
[127] SecurityFocus, March 23, 2004.
[128] SecurityTracker Alert, 1009442, March 16, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[129] ***Oracle updates advisory***[130]	**Windows NT 4.0/2000, XP, Unix, OpenVMS**	**Oracle9i Application Server 1.0.2 .2, 9.0.3 .1, 9.0.3, Enterprise Edition 9.0.1 .4, 9.2 .0.2, Personal Edition 9.0.1 .4, 9.2 .0.2, Standard Edition 9.0.1 .4, 9.2 .0.2**	A remote Denial of Service vulnerability exists when a malicious user passes malformed DTDs (Data Type Definitions) via XML inside of a SOAP (Simple Object Access Protocol) message.	**Patches available via Metalink Document ID 259556.1 located at:** **http://metalink.oracle.com/**	**Oracle 9i Application/ Database Server Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
Oracle[131, 132]	Windows, Unix	Application Server Web Cache 10g 9.0.4.0, Oracle9i Application Server Web Cache 2.0.0.4, 9.0.2 .3, 9.0.2 .2, 9.0.3 .1	Multiple unspecified vulnerabilities exist due to errors when handling client requests, which are remotely exploitable.	Patches available at: http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=265310.1	Oracle Application Server Web Cache Multiple Unspecified	**High**	Bug discussed in newsgroups and websites.
Phorum[133]	Windows, Unix	Phorum 3.1-3.1.2, 3.2-3.2.8, 3.3.1-3.3.2, 3.4-3.4.6, 5.0.3 BETA	A Cross-Site Scripting vulnerability exists in the 'login.php,' 'register.php,' and 'profile.php' modules due to insufficient sanitization of the 'HTTP_REFERER' parameter, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrades available at: http://www.phorum.org/downloads/phorum-3.4.7.tar.gz	Phorum Multiple Module Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[129] Oracle Security Alert 65, February 18, 2004.

[130] Oracle Security Alert 65, Mach 12, 2004.

[131] Oracle Security Alert 66, March 6, 2004.

[132] VU#413006, https://www.kb.cert.org/vuls/id/413006.

[133] SecurityTracker Alert, 1009433, March 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpBB Group[134]	Windows, Unix	phpBB 1.0.0, 1.2.0, 1.2.1, 1.4.0-1.4.2, 1.4.4, 2.0.0, 2.0 Beta 1, 2.0 RC1-RC4, 2.0.1-2.0.6	A vulnerability exists in the 'search.php' script when 'register_global' is set to 'on, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBB 'Search.PHP' SQL Command Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
phpBB Group[135]	Windows, Unix	phpBB 1.0 .0, 1.2.0-1.2.1, 1.4.0-1.4.2, 1.4.4, 2.0.0, 2.0 Beta 1, 2.0 RC1-RC4, 2.0.1-2.0.7	Input validation vulnerabilities exists in the 'admin_smilies.php' and 'admin_styles.php' scripts, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	phpBB Multiple Input Validation Vulnerabilities	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
phpBB Group[136] ***Upgrade now available*** [137]	**Windows, Unix**	**phpBB 2.0 .0, 2.0 RC4, 2.0.1-2.0.7**	**A Cross-Site Scripting vulnerability exists in 'viewtopic.php' due to insufficient verification of the 'postorder' parameter, which could let a remote malicious user execute arbitrary HTML or script code.**	***Upgrade available at:*** **http://www.phpbb.com/downloads.php**	**PHPBB ViewTopic. PHP Cross-Site Scripting**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.**
phpBB Group[138]	Windows, Unix	phpBB 2.0.6 c	A vulnerability exists in the 'admin_smilies.php' and 'admin_styles.php' scripts due to insufficient validation of the 'id' parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PhpBB Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[134] SCAN Associates Sdn Bhd Security Advisory, March 14, 2004.
[135] GulfTech Security Research Team Advisory, March 21, 2004.
[136] Bugtraq, February 28, 2004.
[137] Bugtraq, March 1, 2004.
[138] GulfTech Security Research Team Advisory, March 20, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpBB Group[139]	Windows, Unix	phpBB 2.0 .0, 2.0 RC1-RC4, 2.0.1-2.0.6, 2.0.6 c, 2.0.6 d	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'viewtopic.php' and 'viewforum.php' scripts due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists in the 'search.php' script due to insufficient verification of the 'search_results' parameter, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.phpbb.com/downloads.php	PHPBB Cross-Site Scripting & SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group[140]	Windows, Unix	phpBB 2.0.6 d	A Cross-Site Scripting vulnerability exists in the 'profile.php' script due to insufficient verification of the 'avatarselect' parameter, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade available at: http://prdownloads.sourceforge.net/phpbb/phpBB-2.0.8.zip?download	phpBB 'profile.php' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Phpnuke. org [141]	Windows, Unix	Error Manager PHP-Nuke Module 2.1	Multiple vulnerabilities exist: a vulnerability exists in 'error.php' due to insufficient verification of the 'newlang,' 'lang,' and 'language' parameters, which could let a remote malicious user execute arbitrary HTML or script code; a vulnerability exists in 'error.php' due to insufficient verification of the 'pagetitle' parameter, which could let a remote malicious user execute arbitrary HTML or script code; a vulnerability exists in 'error.php' due to insufficient verification of the 'error parameter, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists due to insufficient verification of the parameters logged by Error Manager, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHP-Nuke Error Manager Module Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concept exploits have been published.

[139] Secunia Advisory, SA11121, March 15, 2004.
[140] SecurityTracker Alert, 1009519, March 23, 2004.
[141] waraxe-2004-SA#010, March 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHPX[142] ***Exploit scripts published*** [143]	**Multiple**	**PHPX 3.2.3**	**Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'main.inc.php,' and 'help.inc.php' scripts, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the subject field in Personal Messages and Forum, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because it is possible to edit the PXL parameter in the cookie, which could let a remote malicious user obtain administrative access.**	**Update available at:** **http://sourceforge.net/project/showfiles.php?group_id=67670**	**PHPX Multiple Vulnerabil-ities**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Produc-tive Computer Insight[144]	Windows	Net Support School 7.0	A password encryption vulnerability exists due to a failure of the application to protect passwords with a sufficiently affective encryption scheme, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NetSupport School Weak Password Encoding	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
ReGet Software [145]	Windows	ReGet Deluxe 3.0 build 121	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ReGet Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Rob J. Meijer[146]	Unix	rident.pl 0.91 b	A vulnerability exists because 'rident.pl' uses a temporary file ('/tmp/rident.pid') in an unsafe manner, which could let a malicious user modify sensitive information.	No workaround or patch available at time of publishing.	rident.pl File Override	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Shamit Bagchi [147]	Unix	XWeb 1.0	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	Patch available at: http://in.geocities.com/shamit_bagchi/download.html	XWeb Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

[142] Bugtraq, February 3, 2004.
[143] SecurityFocus, March 16, 2004.
[144] SecurityTracker Alert, 1009556, March 26, 2004.
[145] SecurityFocus, March 22, 2004.
[146] SecurityTracker Alert, 1009552, March 24, 2004.
[147] Secunia Advisory, SA11186, March 23, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Squid Guard[148]	Unix	Squid Guard 1.0.0, 1.1.0-1.1.5, 1.2.0	A vulnerability exists due to a failure to filter out invalid URIs, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	SquidGaurd NULL URL Character Unauthorized Access	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SSH Communications[149, 150]	Unix	SSH Tectia Server 4.0.3, 4.0.4	A vulnerability exists in the password change mechanism that executes the 'passwd' program during user authentication to change the user's password when the user's password has expired, which could let a remote malicious user obtain sensitive information.	Upgrades available at: http://www.ssh.com/support/downloads/tectia-server-unix/updates-and-packages-4-0.html	SSH Tectia Server Private Key Disclosure	Medium	Bug discussed in newsgroups and websites.
SteelID[151]	Windows NT	thePhoto Tool	A vulnerability exists in the 'login.asp' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SteelID thePhotoTool Login.ASP SQL Injection	**High**	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc.[152]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists in the 'vfs_getvfssw()' function due to insufficient sanitization, which could let a malicious user obtain root access.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris 'vfs_getvfssw' function Root Access	**High**	Bug discussed in newsgroups and websites.
Sybari Software[153]	Windows NT, Unix	Antigen for Lotus Domino 7.0 Build 722 (SR2)	A remote Denial of Service vulnerability exists due to an error in a filter used for detecting encrypted variants of the Bagel virus.	Upgrade available at: http://www.sybari.com/download/licensed.asp	Sybari AntiGen For Lotus Domino Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[154]	Multiple	Norton Internet Security 2004, Professional Edition, Personal Firewall 2004	A remotely-exploitable vulnerability exists that allows an anonymous malicious user to execute a Denial of Service attack against systems running default installations	No workaround or patch available at time of publishing.	Internet Security/ Personal Firewall Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[148] SecurityFocus, March 19, 2004.
[149] Secunia Advisory, SA11193, March 23, 2004.
[150] VU#814198, https://www.kb.cert.org/vuls/id/814198.
[151] Securiteam, March 15, 2004.
[152] SecurityFocus, March 23, 2004.
[153] Secunia Advisory, SA11120, March 15, 2004.
[154] eEye Digital Security Advisory, EEYEB-20040309, March 9, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec[155, 156]	Windows	Norton Internet Security 2004, 2004 Professional Edition	A vulnerability exists in the 'LaunchURL' method in the 'WrapNISUM Class' (WrapUM.dll) ActiveX Component, which could let a remote malicious user execute arbitrary code.	A patch is available via the LiveUpdate feature.	Norton Internet Security 'WrapNISUM' Class Remote Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[157, 158]	Windows	Norton AntiSpam 2004	A buffer overflow vulnerability exists due to a boundary error within the 'SymSpamHelper Class' (symspam.dll) ActiveX component, which could let a remote malicious user execute arbitrary code.	A patch is available via the LiveUpdate feature.	Norton AntiSpam 'SymSpam Helper' Class Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Tarantella Inc.[159]	Unix	Tarantella Enterprise 3 3.40	A Cross-Site Scripting vulnerability exists in the 'ttacab.cgi' script due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.tarantella.com/tarantella_downloads/Tarantella.E3/cgi.605393/ttaarchives.cgi.gz	Tarantella Enterprise 3 Remote Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Tarantella Inc. [160]	Unix	Tarantella Enterprise 3 3.0 1, 3.0, 3.10, 3.11, 3.20, 3.30, 3.40	A Cross-Site Scripting vulnerability exists in the 'ttaarchives.cgi' script due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.tarantella.com/tarantella_downloads/Tarantella.E3/cgi.605393/ttaarchives.cgi.gz	Tarantella Enterprise 3 Remote Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Techland[161]	Windows	Chrome 1.2 .0	A remote Denial of Service vulnerability exists due to a failure to validate input of data received via network communications.	No workaround or patch available at time of publishing.	Techland Chrome Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Texas Imperial Software[162]	Windows	WFTPD 3.21 R1&R2, WFTPD Pro 3.21 R1&R2	A remote Denial of Service vulnerability exists due to an error in the handling of various FTP command arguments.	Upgrades available at: http://www.wftpd.com/downloads/32wfd321.zip	WFTPD Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[155] NGSSoftware Insight Security Research Advisory, NISR19042004b, March 19, 2004.

[156] VU#549054, https://www.kb.cert.org/vuls/id/549054.

[157] NGSSoftware Insight Security Research Advisory, NISR19042004a, March 19, 2004.

[158] VU#344718, https://www.kb.cert.org/vuls/id/344718.

[159] Tarantella Security Bulletin #09, March 16, 2004.

[160] Tarantella Security Bulletin #09, March 16, 2004.

[161] Securiteam, March 24, 2004.

[162] Securiteam, March 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
The XMB Group[163]	Windows, Unix	XMB Forum 1.8 SP3, 1.9 beta	Multiple vulnerabilities exists: a vulnerability exists in the 'forumdisplay.php,' 'member.php,' 'misc.php,' and 'today.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'forumdisplay.php' script due to insufficient validation of user-supplied input in the 'tpp' parameter, which could let a remote malicious user execute arbitrary code; Cross-Site Scripting vulnerabilities exists in the 'xmb.php,' 'editprofile.php' (beta version only), 'u2u.php,' 'stats.php,' 'post.php,' and 'forumdisplay.php' scripts, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists in 'phpinfo.php,' which could let a remote malicious user obtain sensitive information or execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	XMB Forum Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however Proofs of Concept exploits have been published.
Trend Micro[164]	Windows, NT 4.0, 2000, XP, 2003, Unix	InterScan VirusWall for Windows NT 3.4-3.6, 3.51, 3.52, build 1466,	A Directory Traversal vulnerability exists in '/ishttpd/localweb/java/?' due to insufficient verification, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Interscan Viruswall Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Virtual Programming[165]	Windows 95/98/NT 4.0/2000, Unix	VP-ASP 4.0, 4.50, 5.0	A vulnerability exists in the 'catalogid' parameter due to insufficient verification of user supplied input, which could let a remote malicious user execute arbitrary code.	Workaround available at: http://www.vpasp.com/virtprog/info/faq_securityfixes.htm	VP-ASP Shopping Cart 'CatalogID' Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[163] waraxe-2004-SA#012, March 26, 2004.
[164] Securiteam, March 24, 2004.
[165] SecurityFocus, M arch 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
VocalTec Commun-ications [166]	Multiple	VocalTec VGW4/8 Telephony Gateway	A vulnerability exists in the 'home.asp' file which could let a remote malicious user bypass authentication.	No workaround or patch available at time of publishing.	VocalTec VGW4/8 Telephony Gateway Remote Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Warp Speed[167]	Windows, Unix	4nAlbum Module 0.92	Multiple vulnerabilities exist: a vulnerability exists because the ‘displaycategory.php’ script exposes the installation path, which could let a remote malicious user obtain sensitive information; a vulnerability exists in ‘displaycategory.php’ due to insufficient validation of the ‘basepath’ parameter, which could let a local/remote malicious user execute arbitrary code; a Cross-Site Scripting vulnerability exists in ‘nmimage.php’ due to insufficient verification of the ‘z’ parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the ‘gid’ parameter due to insufficient verification before being used in a SQL query, which could let a remote malicious user execute arbitrary SQL code.	No workaround or patch available at time of publishing.	WarpSpeed 4nAlbum Module For PHPNuke Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
xinehq.de [168]	Unix	xine 1-rc3b, 1-rc3a, 1-rc1-rc3, 1-rc0a, 1-beta1-beta12, 0.9.13	A vulnerability exists because the ‘xine-bugreport’ and ‘xine-check’ scripts create temporary files in an insecure manner, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Xine Bug Reporting Script Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[166] Bugtraq, March 15, 2004.
[167] waraxe-2004-SA#006, March 15, 2004.
[168] Bugtraq, March 20, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
YaBB[169]	Windows, Unix	YaBB 1 Gold - SP 1.3, YaBB SE Simple Machines SMF 1.0b, YaBB SE 1.5.1	Multiple Cross-Site Scripting vulnerabilities exist in the 'glow' and 'shadow' tags due to insufficient validation, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrades available at: http://www.simplemachines.org/download.php The vendor has announced that fixes for YaBB SE will not be released, as this product is no longer supported.	YABB/YABB SE Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
YaBB SE[170] ***Upgrade now available*** *[171]*	**Windows, Unix**	**YaBB SE 1.5.4, 1.5.5 b, SE 1.5.5**	**Multiple vulnerabilities exists in the 'ModifyMessage.php' file: a vulnerability exists in the '$msg' parameter due to insufficient validation, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the '$postid' parameter due to insufficient validation, which could let a remote malicious user execute arbitrary commands; and a Directory Traversal vulnerability exists in the '$attachOld' parameter due to insufficient validation, which could let a remote malicious user obtain sensitive information.**	***Upgrade available at:*** **http://www.simplemachines.org/download.php**	**YABB SE Multiple Input Validation Vulnerabil-ities**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concepts have been published.**

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[169] Bugtraq, March 16, 2004.
[170] SecurityTracker Alert, 1009275, March 1, 2004.
[171] Bugtraq, March 17, 2004.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 13 and March 30, 2004, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period 50 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 30, 2004	**mystic2.c**	**Script that exploits the Mythic Entertainment Dark Age of Camelot Encryption Key Signing vulnerability.**
March 29, 2004	557iss_pam_exp.c	Script that exploits the Internet Security Systems Protocol Analysis Module Remote Buffer Overflow vulnerability.
March 26, 2004.	**etherealEIGRPTLV_IP_INTDoS.c**	**Script that exploits the Ethereal Buffer Overflow vulnerabilities.**
March 26, 2004	**invscoutdAIX5l_4xSymLinkExploit.pl**	**Script that exploits the AIX 'invscoutd' Insecure Logfile Handling vulnerability.**
March 26, 2004	**netsupport.txt**	**Exploit for the NetSupport School Weak Password Encryption vulnerability.**
March 26, 2004	**netSupportSchoolWeakPassExpl.pas**	**Exploit for the NetSupport School Weak Password Encryption vulnerability.**
March 26, 2004	**waraxe-2004-SA#012.txt**	**Exploitation information for the XMB Forum Multiple Vulnerabilities.**
March 25, 2004	emil-poc.tar.gz	Proof of Concept exploit for the Emil Multiple Buffer Overflow & Format String vulnerability.
March 25, 2004	**ethboom.zip**	**Proof of Concept exploit for the Etherlords Remote Denial of Service vulnerability.**
March 25, 2004	**etherlords.txt**	**Remote Proof of Concept exploit for Etherlords I & II Denial of Service vulnerability.**
March 25, 2004	MSWordPW.txt	Information on how to bypass Password protection on Microsoft Word documents with step by step instructions given.
March 25, 2004	rkhunter-1.0.1.tar.gz	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
March 25, 2004	**vz012004-esignal7.txt**	**Exploit for the ESignal Remote Buffer Overflow vulnerability.**
March 25, 2004	**vz-eSignal76.pl**	**Perl script that exploits the ESignal Remote Buffer Overflow vulnerability.**
March 24, 2004	picobof.zip	Proof of Concept exploit for PicoPhone Buffer Overflow Logging Function vulnerability.
March 24, 2004	picophone163.txt	Exploit for PicoPhone Buffer Overflow Logging Function vulnerability.
March 24, 2004	picophoneExploit.zip	Exploit for the PicoPhone Internet Phone Remote Buffer Overflow vulnerability.
March 23, 2004	**darkAgeOfCamelotMITMexploit.c**	**Script that exploits the Mythic Entertainment Dark Age of Camelot Encryption Key Signing vulnerability.**
March 23, 2004	**FromEmailHeaderExpl.c**	**Script that exploits the Foxmail Remote Buffer Overflow vulnerability.**
March 23, 2004	**ragefreeze.zip**	**Exploit for The Rage Game Server Remote Denial of Service vulnerability.**
March 23, 2004	**terminator3.txt**	**Exploit for the Clever's Games Terminator 3: War of the Machines Remote Client Buffer Overflow vulnerability.**
March 23, 2004	**therage101.txt**	**Exploit for The Rage Game Server Remote Denial of Service vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 23, 2004	**wsftp_allo.cpp**	**Script that exploits the WS_FTP 'Allo' Buffer Overflow Vulnerability.**
March 23, 2004	**wsftp_stat.cpp**	**Script that exploits the WS_FTP 'STAT' Buffer Overflow Vulnerability.**
March 23, 2004	**wsftp402eval.txt**	**Exploit for the IpSwitch WS_FTP Buffer Overflow vulnerability.**
March 23, 2004	**wsftp402eval3.txt**	**Exploit for the IpSwitch WS_FTP Buffer Overflow vulnerability.**
March 23, 2004	**wsftp402eval4.txt**	**Exploit for the IpSwitch WS_FTP Buffer Overflow vulnerability.**
March 23, 2004	**xp_ws_ftp_server.zip**	**Exploit for the IpSwitch WS_FTP Buffer Overflow vulnerability.**
March 23, 2004	**xp_ws_ftp_server2.zip**	**Exploit for the IpSwitch WS_FTP Buffer Overflow vulnerability.**
March 19, 2004	**chrome1200.txt**	**Exploit for the Techland Chrome Remote Denial of Service vulnerability.**
March 19, 2004	eudora603.pl	Exploit that performs an attachment spoofing demo for Eudora.
March 19, 2004	smbprintsymlink.txt	Exploit for the smbprint vulnerability.
March 19, 2004	**t3cbof.zip**	**Script that exploits the Clever's Games Terminator 3: War of the Machines Remote Client Buffer Overflow vulnerability.**
March 18, 2004	**chromeboom.zip**	**Proof of Concept exploit for the Techland Chrome Remote Denial of Service vulnerability.**
March 18, 2004	eckbox-v0.9.3.tar.gz	Eckbox is van Eck phreaking software that interprets a radio signal emanating from a computer's monitor to recreate the image (in black and white) that is displayed on it.
March 18, 2004	mimedefang-2.41.tar.gz	A flexible MIME e-mail scanner.
March 17, 2004	**ex_getlvcb_aix433_limited.pl**	**Proof of Concept exploit for the AIX Getlvcb Command Line Argument Buffer Overflow vulnerability.**
March 17, 2004	**ex_putlvcb_aix433_limited.pl**	**Proof of Concept exploit for the AIX 'Putlvcb' Utility Buffer Overflow vulnerability.**
March 17, 2004	secureftp_poc.pl	Proof of Concept exploit for the GlobalSCAPE Secure FTP Server SITE Command Remote Buffer Overflow vulnerability.
March 17, 2004	WFTPD-GuiDoS.pl	Proof of Concept exploit for the WFTPD Server GUI Remote Denial Of Service vulnerability.
March 17, 2004	**x_make_aix433_limited.pl**	**Proof of Concept exploit for the GNU Make For IBM AIX CC Path Local Buffer Overflow vulnerability.**
March 16, 2004	**crafty.zip**	**Exploit for the Crafty 'crafty.bin' Buffer Overflow vulnerability.**
March 16, 2004	phpx324.txt	Exploit for the PHPX Insecure Management Session vulnerability.
March 16, 2004	phpxSessHijackPOC.php	Exploit for the PHPX Session Hijack vulnerability.
March 15, 2004	**firew0rker.c**	**Script that exploits the Media Services MX_STATS_\LogLine NSIISlog.DLL Remote Buffer Overflow vulnerability.**
March 15, 2004	**gemuruh-v2.php.txt**	**Proof of Concept exploit for the PHPBB Search.PHP Search_Results Parameter SQL Injection vulnerability.**
March 15, 2004	mathopdExploit.c	Script that exploits the MathoPD Remote Buffer Overflow vulnerability.
March 15, 2004	**mdaemon-exploit.c**	**Script that exploits the MDaemon/ WorldClient 'Form2Raw' Remote Buffer Overflow vulnerability.**
March 15, 2004	**phpBB206a.txt**	**Exploit for the PHPBB 'Search.PHP' SQL Command Injection vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 13, 2002	hydra-3.1.tar.gz	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more. Includes SSL support, parallel scans, and is part of Nessus.

Trends

- **There are a number of pieces of malicious code spreading on the Internet through e-mail attachments, peer-to-peer file sharing networks and known software vulnerabilities. Current threats include the Phatbot Trojan Horse, W32/Beagle Virus, W32/Netsky Virus, and the W32/MyDoom Virus. For more information, see Cyber Security Alert SA04-079A located at:** http://www.us-cert.gov/cas/alerts/SA04-079A.html**.**
- **A virus known as the "Witty" worm is spreading over the Internet and has damaged computers worldwide. It exploits the Internet Security Systems Protocol Analysis Module Remote Buffer Overflow vulnerability (see entry in 'Bugs, Holes, & Patches table. For more information about this worm, see WORM_WITTY.A entry (item is boldfaced/red) in the Virus Section below.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. NOTE: At times, viruses may contain names or content that may be considered offensive.

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

W32/Agobot-ED (Aliases: Backdoor.Agobot.3.gen, W32/Gaobot.worm.gen.d) (Win32 Worm): This is a network worm that also allows unauthorized remote access to the computer via IRC channels. It tries to copy itself to network shares with weak passwords. W32/Agobot-ED copies itself to the Windows system folder as FILENAME.EXE and creates entries in the registry at the following locations to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Configuration Loader
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Configuration Loader

The worm disables the shares C$, D$, ADMIN$, and IPC$. W32/Agobot-ED attempts to terminate various virus, anti-virus, and security processes. It listens on a particular port and supplies a copy of the worm in response to incoming connections.

W32/Agobot-EF (Alias: Backdoor.Agobot.3.gen) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-EF copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. When first run, W32/Agobot-EF copies itself to the Windows system folder with the filename explore.exe and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Monitor = explor.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Monitor = explor.exe

W32/Agobot-EF also registers itself as a service which will be activated when Windows starts up. The name of the service is Monitor. It connects to a remote IRC server and joins a specific channel. The backdoor functionality of the worm can then be accessed by a malicious user using the IRC network. The worm also attempts to terminate and disable various security-related programs.

W32/Agobot-EX (Aliases: Backdoor.Agobot.hm, WORM_AGOBOT.HM, W32.HLLW.Polybot, Phatbot, W32/Polybot.l!irc, WORM_AGOBOT.HM) (Win32 Worm): This is an IRC backdoor Trojan and network worm. When first run W32/Agobot-EX copies itself to the Windows system folder with the filename soundman.exe. The following registry entries are created with the intention of starting the worm when a user logs into Windows, but an error results in these values being garbage:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\^`d}qZxu= ~`d}qzxu3zYF
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\^`d}qZxu= ~`d}qzxu3zYF

W32/Agobot-EX also registers itself as a service which will be activated when Windows starts up. The name of the service is SoundMan. It connects to a remote IRC server and joins a specific channel. The backdoor functionality of the worm can then be accessed by a malicious user using the IRC network. A malicious user can issue commands to start the worm scanning for vulnerable computers to copy itself to. The worm also attempts to terminate and disable various security-related programs.

W32/Agobot-FG (Alias: Backdoor.Agobot.3.gen) (Win32 Worm): This is a network aware worm that also allows unauthorized remote access to the computer via IRC channels. W32/Agobot-FG tries to copy itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. W32/Agobot-FG copies itself to the Windows system folder as EXPLORED.EXE and creates entries in the registry at the following locations to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

On NT-based versions of Windows, W32/Agobot-FG tries to create a system service called "mpr" which it sets to run on system startup, creating registry entries in the following locations:

- HKLM\System\CurrentControlSet\Services\MPR
- HKLM\System\CurrentControlSet\Enum\Root\LEGACY_MPR

W32/Agobot-FG attempts to terminate the following virus, anti-virus and security-related processes.

W32/Agobot-FH (Aliases: Backdoor.Agobot.hx, W32/Gaobot.worm.gen.d, Win32/Agobot.3.MQ, W32.HLLW.Gaobot.gen) (Win32 Worm): This worm has been reported in the wild. It is an IRC backdoor Trojan and network worm. W32/Agobot-FH is capable of spreading to computers on the local network protected by weak passwords. When first run W32/Agobot-FH copies itself to the Windows system folder as soundconf.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Video Proes = winaii.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Video Proes= winaii.exe

W32/Agobot-FH also registers itself as a service which will be activated when Windows starts up. The name of the service is Video Proes. Each time W32/Agobot-FH is run, it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-FH then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-FH attempts to terminate and disable various anti-virus and security-related programs.

W32/Bagle-HTML (Alias: HTML_BAGLE.Q1) (Win32 Worm): This worm has been reported in the wild. It is the e-mail sent by W32/Bagle-Q and W32/Bagle-R. The e-mail attempts to launch an exploit, described in Microsoft Security Bulletin MS03-040, in order to automatically download and run the worm from a number of compromised computers.

W32/Bagle.p@MM (Aliases: PE_BAGLE.P, Bagle.P) (Win32 Worm): This new BAGLE variant is very similar to PE_BAGLE.N but bigger in actual size. It propagates via e-mail with varying subjects, message bodies, and attachment file names. This virus searches for files with certain extension names, from which it gathers target recipients. Using its own SMTP (Simple Mail Transfer Protocol) engine, it sends out e-mail messages with spoofed return addresses and itself as attachment. It also spreads by dropping files in folders that have the text string "shar," for example, C:\Program Files\KaZaA\My Shared Folder. At every execution, this virus infects Win32 executable files (.EXE) in randomly selected folders in all fixed drives. It does this by attaching its malicious code, adding another section at the end of the file. It opens TCP port 2556 and waits for incoming commands from a remote user, who must send specially–crafted data or packets to be able to command this virus. This virus attempts to prevent the automatic execution of NETSKY variants by deleting certain registry entries. It also has the ability to terminate certain processes, most of which are related to antivirus and firewall applications. It removes its autostart registry entries on December 31, 2005 and on any latter date, practically uninstalling itself and leaving it unable to run as Windows startup. This UPX-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP. It uses the icon for true-type fonts.

W32/Bagle-Q (Alias: Win32/Bagle.Q) (Win32 Virus): This virus has been reported in the wild. It is a mass-mailing virus that spreads in an unusual manner. W32/Bagle-Q spreads via a "carrier" e-mail which does not contain the worm as an attachment. The e-mail sender address is spoofed, the subject line is randomly chosen, and there is no visible message text. The e-mail addresses are harvested from the hard drive of infected machines by searching for files with the extensions WAB, TXT, MSG, HTM, SHTM, STM, XML, DBX, MBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, WSH, ADB, TBB, SHT, XLS, and OFT. W32/Bagle-Q avoids e-mail addresses containing the following: @hotmail, @msn, @microsoft, rating@, f-secur, anyone@, bugs@, contract@, feste, gold-certs@, help@, info@, nobody@, noone@, kasp, admin, microsoft, support, ntivi, unix, linux, listserv, certific, sopho, @foo, @iana, free-av, @messagelab, winzip, google, winrar, samples, abuse, panda, cafee, spam, @avp., noreply, local, root@, or postmaster@. When you open the "carrier" e-mail, the e-mail attempts to exploit a vulnerability in Outlook. The exploit may cause the e-mail client to automatically download W32/Bagle-Q from the IP address of a computer infected with a Bagle variant. The IP address of the computer "server" serving the Bagle executable is randomly chosen from the list of of 590 IP addresses from the virus data section. The security vulnerability was reportedly patched by Microsoft in Microsoft Security Bulletin MS03-040. The "carrier" e-mail connects to port 81 of the host and opens an HTML file. The HTML file drops and launches a Visual Basic script q.vbs. This script connects to the same server and downloads W32/Bagle-Q via an HTTP (web) request to TCP port 81. The downloaded copy of W32/Bagle-Q is placed into your system folder with the name directs.exe or direct.exe (depending on the variant). W32/Bagle -Q loads on your PC and terminates a wide range of security applications. A registry entry is added to the following key so that the program directs.exe loads every time you logon to your computer:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

W32/Bagle-Q makes multiple copies of itself into folders which are likely to be part of a file-sharing network. It infects programs on your PC by appending itself to existing EXE files.

W32/Bagle-R (Aliases: Win32/Bagle.R, W32/Bagle.R.worm, W32/Bagle.S, I-Worm.Bagle.p, W32/Bagle.T, W32.Beagle.R@mm, W32.Beagle.S@mm, W32.Beagle.T@mm, 32/Bagle.S.1, I-Worm/Bagle.S, I-Worm.Win32.Bagle.Q, I-Worm.Bagle.r, Win32.HLLM.Beagle.49152, Win32:Beagle-S) (Win32 Virus): This virus has been reported in the wild. It is a mass-mailing virus that spreads in an unusual manner. W32/Bagle-R spreads via a "carrier" e-mail which does not contain the worm as an attachment. The e-mail sender address is spoofed, the subject line is randomly chosen, and their is no visible message text. The e-mail addresses are harvested from the hard drive of infected machines by searching for files with the extensions WAB, TXT, MSG, HTM, SHTM, STM, XML, DBX, MBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, WSH, ADB, TBB, SHT, XLS, and OFT. W32/Bagle-R avoids e-mail addresses containing the following: @hotmail, @msn, @microsoft, rating@, f-secur, anyone@, bugs@, contract@, feste, gold-certs@, help@, info@, nobody@, noone@, kasp, admin, icrosoft, support, ntivi, unix, linux, listserv, certific, sopho, @foo, @iana, free-av, @messagelab, winzip, google, winrar, samples, abuse, panda, cafee, spam, @avp., noreply, local, root@, or postmaster@. When you open the "carrier" e-mail, the e-mail attempts to exploit a vulnerability in Outlook. The exploit may cause the e-mail client to automatically download W32/Bagle -R from the IP address of a computer infected with a Bagle variant. The IP address of the computer "server" serving the Bagle executable is randomly chosen from the list of 590 IP addresses from the virus data section. The security vulnerability was reportedly patched by Microsoft in Microsoft Security Bulletin MS03-040. The "carrier" e-mail connects to port 81 of the host and opens an HTML file. The HTML file drops and launches a Visual Basic script q.vbs. This script connects to the same server and downloads W32/Bagle-R via an HTTP (web) request to TCP port 81. The downloaded copy of W32/Bagle-R is placed into your system folder with the name directs.exe or direct.exe (depending on the variant). W32/Bagle -R loads on your PC and terminates a wide range of security applications. A registry entry is added to the following key so that the program directs.exe loads every time you logon to your computer:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

W32/Bagle-R makes multiple copies of itself into folders which are likely to be part of a file-sharing network. W32/Bagle-R infects programs on your PC by appending itself to existing EXE files.

W32.BAGLE.T@MM (Aliases: PE_BAGLE.T, W32.BEAGLE.T@MM, BAGLE.T) (Win32 Worm): Like recent BAGLE variants, this malware also infects files. Its distinct feature is the use of a known vulnerability to propagate. Besides sending itself as e-mail attachment to target addresses it gathers from the infected system, this virus also exploits a known vulnerability in order to increase its chances of spreading. It sends an e-mail that exploits the Object Tag vulnerability in Popup Window (MS03-040), which allows a malicious user to run arbitrary code on a user's system. The e-mail message it sends for this particular e-mail propagation routine does not have an attachment but a link to the virus copy. When viewed, this e-mail attempts to download PE_BAGLE.T from a certain location. More information about the vulnerability is available from the following Microsoft page: http://www.microsoft.com/technet/security/bulletin/MS03-040.mspx. This virus also has backdoor capabilities. It opens port 2556 and other randomly-generated ports, where it waits for commands from a malicious user. It terminates certain processes, most of which are related to antivirus and firewall applications. It runs on Windows 95, 98, ME, NT, 2000 and XP.

W32/Bagle-U (Aliases: W32.Beagle.gen, Bagle.U, WORM_BAGLE.U, W32.Beagle.U@mm, W32/Bagle.u@MM , Win32.Bagle.U) (Win32 Worm): This worm has been reported in the wild. It is a member of the W32/Bagle family of worms. The worm starts the mshearts application on the system when active. In order to run automatically when Windows starts up, the worm copies itself to the file gigabit.exe in the Windows system folder and sets the following registry entry to point to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\gigabit.exe

W32/Bagle-U also creates the following registry entries:

- HKCU\Software\Windows2004\gsed
- HKCU\Software\Windows2004\fr1n

The worm listens on port 4751 and sends registration information containing this port number to a remote web site. This port can be used by a remote malicious user to update the worm. The uploaded file will be dropped as a random EXE filename starting with the string 'bsud' into the Windows folder and executed. If the file was dropped successfully the original worm file will be deleted. W32/Bagle-U scans all fixed drives recursively for WAB, TXT, MSG, HTM, SHTM, STM, XML, DBX, MBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, WSH, ADB, TBB, SHT, XLS, OFT, UIN, CGI, MHT, DHTM, and JSP files, extracts e-mail addresses from them and sends itself as an attachment to the found addresses. E-mail addresses belonging to the domains AVP and Microsoft are skipped. The e-mails send by the worm have an empty subject line and no message text and the attachment file names are random strings with an EXE extension. The sender address is spoofed and chosen from the list of addresses found on the system. After the end of 2004, the worm will remove itself from the system.

W32/Bagle-V (Aliases: W32.Beagle.U@mm, W32/Bagle.u@MM, Win32/Bagle.V@mm, I-Worm.Bagle.t, W32/Bagle.V@mm, Win32:Beagle-U, Worm/Bagle.U.2, WORM_BAGLE.V) (Win32 Worm): This worm has been reported in the wild. It is a member of the W32/Bagle family of worms. When first run, the worm attempts to run an application called dreder.exe. In order to run automatically when the user logs on to the computer the worm copies itself to the file sysinfo.exe in the Windows system folder and creates the following registry entry:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\sysinfo.exe

W32/Bagle-V also creates the following registry entries:

- HKCU\Software\Windows2005\gsed
- HKCU\Software\Windows2005\fr1n

W32/Bagle-V scans all fixed drives recursively for files with extensions WAB, TXT, MSG, HTM, SHTM, STM, XML, DBX, MBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, WSH, ADB, TBB, SHT, XLS, OFT, UIN, CGI, MHT, DHTM, and JSP, harvests e-mail addresses from them and sends itself as an attachment to the addresses extracted. E-mail addresses belonging to the domains AVP and Microsoft are avoided. The e-mails sent by the worm have an empty subject line and no message text. The attached file is called game.exe. The sender address is spoofed (chosen from addresses found on the system). The worm listens on TCP port 4751 and sends registration information containing this port number to a remote web site. This port can be used by a remote malicious user to update the worm. The uploaded file will be dropped as a random EXE filename starting with the string "bsud" into the Windows folder and executed. If the update is successful the original worm file is deleted. After the end of 2004, the worm will remove itself from the system.

W32.Dinfor.D.Worm (Win32 Worm): This is a variant of W32.Dinfor.Worm, which spreads across network shares and exploits weak passwords. This worm also acts as a backdoor, connecting to an IRC channel and allowing a remote malicious user to control an infected computer.

W32.Gaobot.SA (Aliases: W32.HLLW.Polybot.B, Phatbot, **W32/Gaobot.worm.gen.d) (Win32 Worm):** This is a worm that attempts to spread through network shares that have weak passwords and allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

W32.Hesi.Worm (Visual Basic Worm): This is a Visual Basic (VB) worm that copies itself to remote drives. When W32.Hesi.Worm is executed, it copies itself as %System%\MSDOS.sys and attempts to copy itself to the following drives:

- C:\desktop.sys
- D:\desktop.sys
- E:\desktop.sys
- F:\desktop.sys

If the copy is successful, the worm will create the file, autorun.inf, which allows the worm to be executed when you access the drive. The worm may enumerate open network shares and copy itself as:

- ASDdll.exe

It may also attempt to download the following file: http://whost.home.icq.com/index.files/D.htm

W32.HLLW.Antinny.G (Win32 Worm): This is a variant of W32.HLLW.Antinny. It spreads using the Winny file-sharing network. The worm steals personal information, including name, e-mail and files, and sends it to a file-sharing network. The worm has the Notepad icon or a Windows folder icon.

W32.HLLW.Donk.L (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from a malicious user. The worm attempts to terminate the processes of various antivirus and security related programs.

W32.HLLW.Leox.B (Win32 Worm): This is a variant of W32.HLLW.Leox. It is a worm that sends a URL using QQ, a Chinese instant messaging program. The URL points to a site that hosts the worm. The worm also e-mails password and equipment information from the game, Legend of Mir, to an e-mail address at tom.com.

W32.HLLW.RedDw@mm (Win32 Worm): This is a worm that spreads by e-mail using Microsoft Outlook, mIRC, or by peer-to-peer file sharing. The scripts, which this worm drops, are detected as BAT.RedDw@mm.

W32.HLLW.Gaobot.RF (Win32 Worm): This is a variant of W32.HLLW.Gaobot.gen. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.

W32/Lovero.worm (Win32 Worm): This The binary file's icon is of a deceiving Notepad text type. The malicious file failed to execute properly on a lot of test machines. When it does run successfully, it displays an empty Notepad window. It copies itself, for example on a win2000 system, to the location:

- C:\winnt\system32\syssrv.exe.

To have the file execute automatically at system start it creates a standard registry entry under:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- Name : syssrv
- Data : C:\winnt\system32\syssrv.exe

The process is visible in the Windows Task manager and can also be killed manually. While the malicious process is running, the registry editor can be started but it is not fully functional, the registry information can not be viewed/edited. It also creates a file called Hallo.Roro.htt, having shr file attributes, so it set them to system files, hidden and read-only. The file is a harmless text file in which the virus author expresses his love for someone. The worm tries to copy itself to floppy drives A:. During testing this didn't function very well resulting in a hanging, not responding floppy drive. It doesn't perform mass-mailing. When the payload activates, it might change the autoexec.bat to delete files from the Program Files and Windows folders on the next startup, displaying Indonesian messages.

W32/Lovgate-X (Aliases: I-Worm.LovGate.q, Win32/Lovgate.X, WORM_LOVGATE.Q, W32/Lovgate.q@MM, W32/Sluter.worm.gen, I-Worm.Win32.Lovgate.114176, I-Worm/Lovgate.N) (Win32 Worm): This is a worm with the backdoor functionality that spreads via e-mail, network shares with weak passwords and file sharing networks. W32/Lovgate-X may arrive in the e-mail with a various subject lines, message text, and attachments. When executed, W32/Lovgate-X creates the service "NetMeeting Remote Sharing," copies itself to the Windows folder with the filename Systra.exe and to the Windows system folder with the filenames iexplore.exe, Winexe.exe, avmond.exe, WinHelp.exe , and Kernel66.dll. W32/Lovgate-X extracts the backdoor components to the Windows system folder as ODBC16.DLL, msjdbc11.dll, and MSSIGN30.DLL. In order to run automatically when Windows starts up, W32/Lovgate-X creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\SystemTra = C:\WINDOWS\SysTra.EXE
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VFW Encoder/Decoder Settings = "RUNDLL32.EXE MSSIGN30.DLL ondll_reg"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Program In Windows = "C:\\WINDOWS\\System32\\IEXPLORE.EXE"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Protected Storage = "RUNDLL32.EXE MSSIGN30.DLL ondll_reg"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\runServices\
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\runServices\SystemTra = "C:\\WINDOWS\\SysTra.EXE"HKU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run = "RAVMOND.exe"
- HKCR\exefile\shell\open\command = C:\WINDOWS\System\winexe.exe

W32/Lovgate-X may change the win.ini file by adding path to the Ravmond.exe to the 'run=' line. W32/Lovgate-X attempts to terminate a number of processes. W32/Lovgate-X copies itself to the share folders of file sharing networks. W32/Lovgate-X copies itself to the share folder of the KaZaA network with various filenames.

W32/Lovgate-Z (Aliases: Win32/Lovgate.V, I-Worm.LovGate.r, WORM_LOVGATE.N) (Win32 Worm): This worm has been reported in the wild. It is a variant of the W32/Lovgate family of worms that spread via e-mail, network shares, and file sharing networks. W32/Lovgate-Z copies itself to the Windows system folder as the files WinHelp.exe, iexplore.exe, kernel66.dll and ravmond.exe and to the Windows folder as systra.exe. The worm also drops the files msjdbc11.dll, mssign30.dll, and odbc16.dll which are backdoor components of the worm and provide unauthorized remote access to the computer over a network. The worm drops ZIP files containing a copy of the worm onto accessible drives. The ZIP file may have a RAR extension. The name of the packed file is chosen. The name of the archived file is either PassWord, e-mail or book with an extension of EXE, SCR, PIF or COM. In order to run automatically when the user logs on to the computer W32/Lovgate-Z creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Program In Windows=<Windows system>\IEXPLORE.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinHelp=<Windows system>\WinHelp.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\SystemTra=<Windows>\SysTra.EXE
- HKU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run=RAVMOND.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Protected Storage=RUNDLL32.EXE MSSIGN30.DLL ondll_reg
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VFW Encoder/Decoder Settings=RUNDLL32.EXE MSSIGN30.DLL ondll_reg

W32/Lovgate-Z changes the entry in the registry at the following location to run itself before files with an EXE extension:

- HKCR\exefile\shell\open\command

W32/Lovgate-Z may also change WIN.INI to run itself on system restart. In addition W32/Lovgate-Z copies itself to the file command.exe in the root folder and creates the file autorun.inf there containing an entry to run the dropped file upon system startup. W32/Lovgate-Z spreads by e-mail. E-mail addresses are harvested from WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB, and PL files found on the system. E-mail has various subject lines, message text, and attachments. The worm attempts to reply to e-mails found in the user's inbox using the various filenames as attachments. W32/Lovgate-Z copies itself to the shared folder of an existing KaZaA installation with various filenames. W32/Lovgate-Z also enables sharing of the Windows media folder and copies itself there using various filenames. The worm attempts to spread by copying itself to mounted shares using various filenames. W32/Lovgate-Z also attempts to spread via weakly protected remote shares by connecting to the admin$ share using a password from an internal list and copying itself as the file NetManager.exe to the system folder on the share. The worm tries passwords from the following list: Guest, Administrator, zxcv, yxcv, xxx, xp, win, test123, test, temp123, temp, sybase, super, sex, secret, pwd, pw123, pw, pc, Password, owner, oracle, mypc123, mypc, mypass123, mypass, love, login, Login, Internet, home, godblessyou, god, enable, database, computer, alpha, admin123, Admin, abcd, aaa, a, 88888888, 2600, 2003, 2002, 123asd, 123abc, 123456789, 1234567, 123123, 121212, 12, 11111111, 110, 007, 00000000, 000000, 0, pass, 54321, 12345, password, passwd, server, sql, !@#$%^&*, !@#$%^&, !@#$%^, !@#$%, asdfgh, asdf, !@#$, 1234, 111, 1, root, abc123, 12345678, abcdefg, abcdef, 888888, 666666, 111111, admin, administrator, guest, 654321, 123456, 321, or 123. After successfully copying the file W32/Lovgate-Z attempts to run it as the service "Windows management network service extension" on the remote computer. W32/Lovgate-Z starts a logging thread that listens on port 6000, sends a notification e-mail to an external address and logs received data to the file C:\Netlog.txt. W32/Lovgate-Z attempts to terminate processes containing various strings. It also overwrites EXE files on the system with copies of itself. The original files are saved with a ZMX extension.

W32/Netsky-P (Aliases: Win32/Netsky.Q, WORM_NETSKY.P, W32.Netsky.Q@mm, Win32/Netsky.P@mm, Worm/NetSky.P, W32/Netsky.P.worm) (Win32 Worm): This worm has been reported in the wild. It is a mass-mailing worm which spreads by e-mailing itself to addresses harvested from files on the local drives. The worm copies itself to the Windows folder as FVProtect.exe and adds the following registry entry to run itself whenever the user logs on to the computer:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Norton Antivirus AV= <Windows>\FVProtect.exe

The worm will also copy itself to various peer-to-peer shared folders. W32/Netsky-P harvests e-mail addresses from files with the following extensions: PL, HTM, HTML, EML, TXT, PHP, ASP, VBS, RTF, UIN, SHTM, CGI, DHTM, ADB, TBB, DBX, SHT, OFT, MSG, JSP, WSH, and XML. The worm has a trigger date of 24th of March 2004, at which time it will attempt to mass mail. E-mails have various subject lines, message texts, and attachments. W32/Netsky-P attempts to delete registry entries which may be set by variants of the W32/Mydoom and W32/Bagle worms. W32/Netsky-P also creates a number of the TMP files in the Windows folder: base64.tmp, zip1.tmp, zip2.tmp, zip3.tmp, zipped.tmp.

W32/Netsky-Q (Aliases: I-Worm.NetSky.r, Win32/Netsky.R, W32.Netsky.Q@mm, WORM_NETSKY.Q) (Win32Worm): This worm has been reported in the wild. It is a mass-mailing worm which spreads by e-mailing itself to addresses harvested from files on local drives. The worm copies itself to the Windows folder as SysMonXP.exe, as well as dropping a DLL file to the Windows folder as firewalllogger.txt. The worm then sets the following registry entry so as to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SysMonXP

The worm tries to delete the following registry entries:

- HKR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32
- HKR\Software\Microsoft\Windows\CurrentVersion\Explorer\PINF
- HKR\System\CurrentControlSet\Services\WksPatch4

The worm also attempts to delete a number of other registry entries but due to a bug in the code it will never succeed. Some of the deleted registry entries relate to the W32/Bagle family of worms. If run from a file other than SysMonXP in the Windows folder the worm will attempt open the file TEMP.EML in notepad in addition to its normal execution. W32/Netsky-Q harvests e-mail addresses from files with the following extensions: EML, TXT, PHP, ASP, WAB, DOC, SHT, OFT, MSG, VBS, RTF, UIN, SHTM, CGI, DHTM, ADB, TBB, DBX, PL, HTM, HTML, JSP, WSH, XML, CFG, MBX, MDX, MHT, NMF, NCH, ODS, STM, XLS, or PPT. W32/Netsky-Q will attempt to mass-mail itself to the harvested addresses on 31st March, 5th April, 12th April, 19th April, and 26th April 2004. The worm tries to send itself in two separate e-mails to each of the addresses, one in plain text and the other in MIME. The subject lines, message texts and attachment filenames are randomly chosen. If sent as a zipped file, the worm will have one of the following filenames inside the zip, followed by a large number of spaces and then a .SCR extension:

- message.eml
- msg.eml
- mail.eml
- data.eml

In the MIME e-mail W32/Netsky-Q can attempt to use an IFRAME exploit in order to execute the attachment even if the receiver chooses not to execute it. W32/Netsky-Q drops itself to the following files in the Windows folder with in a Base64 encoded form, ready to mass-mail itself. W32/Netsky-Q will attempt to launch a Denial of Service attack on the following websites between the 8th and 11th March 2004:

- www.cracks.st
- www.cracks.am
- www.emule-project.net
- www.kazaa.com
- www.edonkey2000.com

All day on the 30th March 2004, W32/Netsky-Q will cause infected machines to emit intermit beeps of random pitch and duration. W32/Netsky-Q an encrypted message.

W32.Nimos.Worm (Alias: W32/Nomis.worm) (Win32 Worm): This is a network-aware worm that captures keystrokes and passwords, and then sends them to the malicious user. This worm is written in Microsoft Visual Basic and is packed with PEBundle and ExeStealth.

W32/Nyxem-A (Aliases: I-Worm.Nyxem, WORM_BLUEWORM.A, W32/Mywife.A.worm, W32/MyWife.a@MM, BlueMoon.A, W32.Blackmal@mm) (Win32 Worm): W32/Nyxem-A is an e-mail worm. It arrives in an e-mail as an attachment with various subject lines, message text, and attachment names. In order to run automatically when Windows starts W32/Nyxem-A adds to the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

When run,W32/Nyxem-A will create the file Media.Temp.Mpeg in the temporary folder and launch Windows Media Player with it. The Mpeg file is actually empty and Media Player will complain that the file format is n't recognized.

W32/Protoride-F (Aliases: Worm.Win32.Protoride.f, W32/Protoride.worm, W32.Protoride.Worm) (Win32 Worm): This is a Windows worm that spreads via network shares. The worm also has a backdoor component that allows unauthorized remote access to the computer via IRC channels. W32/Protoride-F attempts to copy itself to the Windows system folder with the filename rdpty.exe and then set the following registry entry so as to run itself before all EXE files:

- HKCR\exefile\shell\open\command

W32/Protoride-F attempts to copy itself to msupdate.exe in the startup folder of shared network computers. W32/Protoride-F may also set the following registry entry:

- HKLM\Software\BeyonD inDustries\ProtoType[v2]

W32/Protoride-F remains resident, running in the background as a service process and listening for commands from remote users via IRC channels.

W32/Sdbot-GR (Aliases: Backdoor.IRCBot.gen, W32/Sdbot.worm.gen) (Win32 Worm): This is both a backdoor Trojan and network-aware worm which runs in the background as a service process and allows unauthorized remote access to the computer via IRC channels. W32/Sdbot-GR copies itself to the Windows system folder as wintask.exe and creates the following registry entries so that the Trojan is run when a user logs on to Windows:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\winlog
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\winlog
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\winlog
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\winlog
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\winlog

W32/Sdbot-GR remains resident, listening for commands from remote users. If the appropriate commands are received, the worm will begin scanning the internet for network shares with weak administrator passwords and will attempt to copy itself to these shares.

W32/Sober-E (Aliases: WORM_SOBER.E, W32.Sober.E@mm**, W32/Sober.e@MM, Win32.Sober.E, I-Worm.Sober.e) (Win32 Worm):** This worm has been reported in the wild. It is a worm that arrives in an e-mail with various subject lines, message text, and attachments. W32/Sober-E will copy itself to the Windows system folder using a combination of the following words with an EXE extension: sys, host, dir, explorer, win, run, log, 32, disc, crypt, data, diag, spool, service, smss32 and sets the following registry entries to ensure it is run at system logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\<random name>= <SYSTEM>\<random file> %1
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<random name>\<random name> <SYSTEM>\<random file>

where <random file> is the name of the copy of the worm and <random name> is generated using the same word list. W32/Sober-E will also create the following files in the Windows system folder:

- bcegfds.lll
- WinRun32.dll - list of e-mail addresses found on system
- MsHelp32.dat - base64 encoded copy of the worm
- msWord.wrd - base64 encoded ZIP copy of the worm
- zmndpgwf.kxx

The files WinRun32.dll, zmndpgwf.kxx and bcegfds.lll are not malicious and can be deleted. When first run, W32/Sober-E will attempt to open MSPaint.exe. If the worm is unable to find MSPaint.exe, it will display a Windows dialog box with the message "Graphic Modul not found."

W32.Timese.AG (Win32 Worm): This is a worm that displays the date and time on the active window's title bar. It sets itself to run at startup and attempts to copy itself to the floppy disk drive. W32.Timese.AG is written in Visual Basic and is packed with ASPack.

WORM_AGOBOT.BY (Win32 Worm): This polymorphic, memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability

It drops itself as the file HALLOWELT.EXE in the Windows system folder. It attempts to log into systems using a list of user names and passwords. It operates as an Internet Relay Chat (IRC) bot through port 6667, where it listens for malicious commands from a remote user. It terminates antivirus-related programs and steals CD keys of certain game applications. It may also terminate BAGLE and NETSKY variants. This FSG-compressed malware runs on Windows NT, 2000, and XP.

WORM_AGOBOT.JR (Internet Worm): Like the earlier AGOBOT variants, this memory-resident worm takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability

It drops itself as the file SVCHOST2.EXE in the Windows system folder and terminates antivirus-related programs. It is compressed using Exe Stealth and runs on Windows XP.

WORM_AGOBOT.KM (Alias: W32/Gaobot.KM.worm) (Internet Worm): This worm exploits certain vulnerabilities to propagate. It takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator Vulnerability

It also attempts to log on to systems using a list of user names and passwords. It drops a copy of itself into accessible machines. This worm has backdoor capabilities. It executes commands sent in via Internet Relay Chat (IRC) and can be used to launch as Denial of Service attack against specified target sites. It terminates certain antivirus processes and files dropped by other malware. The worm steals the Windows Product ID and the CD keys of popular game applications and runs on Windows 2000 and XP.

WORM_AGOBOT.PS (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It drops itself as the file sys32.exe in the Windows system folder. It attempts to log into systems using a list of user names and passwords. It connects to an Internet Relay Chat (IRC) server and opens a random port where it awaits malicious commands. This malware also terminates processes and steals CD keys of certain game applications. This worm usually arrives compressed twice with ASPACK2 and UPX. It runs on Windows NT, 2000 and XP.

WORM_AGOBOT.RS (Aliases: Phatbot.F, W32.HLLW.Gaobot.RS) (Internet Worm): This worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator Vulnerability

A new feature of this worm is its ability to prevent infected users from upgrading their pattern files for their antivirus software by adding a certain entries in the HOSTS file of their machine. It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antivirus-related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It also launches a distributed Denial of Service attack on several Web sites. This malware runs on Windows NT, 2000 and XP.

WORM_LOVGATE.T (Aliases: Aliases: W32.Lovgate.Gen@mm, W32/Lovgate.t@MM, I-Worm.LovGate.u, Win32/LovGate.Variant.Worm, W32/Lovgate.T.worm, I-Worm/Lovgate.P, I-Worm.Win32.Lovgate.103424) (Internet Worm): This memory-resident worm propagates through network shares by dropping copies of itself using various file names into shared folders with read/write access. This worm also propagates via e-mail by replying to all new messages received in Microsoft Outlook and Outlook Express. The e-mail message it sends has the following characteristics:

- From: <user name>
- To: <Original sender>
- Subject: RE: <Original Subject>

This worm also gathers target e-mail addresses from *.HT* files, which it finds in the following locations:

- current folder
- Windows folder

It then sends an e-mail message (varying details) with itself as attachment to all harvested recipients. This worm also has backdoor functionalities. It is able to open port 20168, obtain system information, and allow remote users to execute commands on the compromised system. It drops several copies of itself, as well as its malware components in specified folders in the system. It also uses various autostart methods and memory-residency techniques. This Aspack-compressed worm runs on Windows NT, 2000 and XP.

WORM_NETSKY.N (Aliases: W32/Netsky.n@MM, W32.Netsky.N@mm, Win32.Netsky.N, NetSky.N) (Internet Worm): This new NETSKY variant propagates via e-mail using its own SMTP engine. The e-mail that it sends out has varying subjects, message bodies, and attachment file names. It gathers e-mail addresses from files with certain extension names. It uses a .TXT file icon and displays a logo of a certain antivirus company to disguise a user. It also attempts to remove various registry keys and entries, most of which are associated with other malware specifically MYDOOM and BAGLE variants. This malware is compiled using Borland Delphi, a high level language, and runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_NETSKY.O (Aliases: W32/Netsky.o@MM, Worm/NetSky.O) (Internet Worm): This new NETSKY variant propagates via e-mail using its own SMTP (Simple Mail Transfer Protocol) engine. The e-mail it sends out has varying subjects, message bodies, and attachment file names. It gathers e-mail addresses from files with certain extension names. This malware is UPX-compressed, and runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_NETSKY.Q (Internet Worm): This worm has been reported in the wild in Japan and China. It uses its own Simple Mail Transfer Protocol (SMTP) engine to propagate via e-mail with varying subjects, message bodies, and attachment file names. It gathers e-mail addresses from files with certain extension names in drives C to Z (except for CD-ROM drives). It also exploits a known vulnerability affecting Internet Explorer involving incorrect MIME Header (MS01-020), which allows the automatic execution of e-mail attachments while an e-mail is read or previewed. More information on this vulnerability is available at:

- http://www.microsoft.com/technet/security/bulletin/MS01-020.mspx

It launches a Denial of Service (DoS) attack on several Web sites from April 8 to 11, 2004. This Petite-compressed malware is written using Microsoft Visual C++, a high-level programming language. It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_RANDBOT.A (Aliases: W32/Randbot.worm, Backdoor.IRCBot.gen) (Internet Worm): This malware has both worm and backdoor functionalities. As a worm, it attempts to propagate via default network-shared folders. It scans for nearby IP addresses within the network and for every IP address it finds, it attempts to copy itself as GT.exe in default NT shares. To access a share, it uses a list of passwords. This malware uses IRC (Internet Relay Chat) for its backdoor functionalities. It connects to a certain IRC server and there waits for commands from the malicious user.

WORM_SDBOT.DX (Internet Worm): This malware has both worm and backdoor functionalities. To spread, this worm drops a copy of itself in accessed shared folders as WINLORD32.EXE. It also attempts a brute force attack by logging on to found machines using a list of user names and passwords. It also has backdoor capabilities. It has a built in IRC (Internet Relay Chat) client engine, which enables this malware to connect to an IRC channel and await commands from a remote user. This worm modifies the Windows registry so that it runs at every system startup, and steals the CD keys of several games. It runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_SDBOT.JC (Internet Worm): This worm propagates via network shares. It drops copies of itself on shares that have full access rights, while on those that have restricted access rights, it attempts to force its way into the system using a list of user names and passwords. It also has backdoor functionalities. It has a built-in Internet Relay Chat (IRC) client engine which enables it to connect to an IRC channel, where it waits for commands from a remote user. This worm steals CD keys of several software.

WORM_SNAPPER.A (Aliases: W32/Snapper@MM, W32.Snapper.A@mm, I-Worm.Snapper, Snapper) (Internet Worm): Using its own SMTP (Simple Mail Transfer Protocol) engine, this worm sends copies of itself to all contacts listed in the user's default Windows Address Book (WAB). The e-mail message it sends out has the following details:

- From: <spoofed>
- Subject: Re:
- Attachment: <blank>

The e-mail may appear empty to the recipient but it actually contains an HTML code that utilizes the Object Tag Exploit, which automatically downloads the BANNER.HTM file from a particular Web site into the system. Trend Micro detects this file as HTML_SNAPPER.A. This malware also terminates certain processes. It modifies the registry to register itself as a Browser Helper Object (BHO).

WORM_WITTY.A (Aliases: Witty, W32.Witty.Worm, W32/Witty.worm) (Internet Worm): This memory-based worm spreads on systems running BlackIce. It does not drop any file nor create any registry entries. It takes advantage of a vulnerability in the ICQ Instant Messaging protocol parsing routines of the ISS Protocol Analysis Module (PAM) component, which may lead to a buffer overflow. For more information regarding this vulnerability, see 'Bugs, Holes & Patches' Table entry, Internet Security Systems Protocol Analysis Module Remote Buffer Overflow. This worm spreads across the network via source port 4000 using UDP packets, which are sent to random destination ports. It sends itself to 20,000 remote machines using randomly-generated IP addresses. It is supposed to open a random physical disk drive and may overwrite a random sector of the affected hard disk. Note that the malware code that executes the attack resides only in the memory of affected BlackIce systems, and there are no file counterparts. Because of this, antivirus file scanners are unable to detect the code and there is no applicable pattern file. All affected BlackIce users to download and install the necessary patch available at: http://www.iss.net/download/.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *NOTE: At times, Trojans may contain names or content that may be considered offensive.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
Backdoor.Cazno	**N/A**	**Current Issue**
Backdoor.Cazno.Kit	**N/A**	**Current Issue**
Backdoor.Danton	**N/A**	**Current Issue**
Backdoor.Domwis	N/A	CyberNotes-2004-04
Backdoor.Gaster	N/A	CyberNotes-2004-01
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
Backdoor.IRC.Aladinz.J	J	CyberNotes-2004-04
Backdoor.IRC.Aladinz.L	L	CyberNotes-2004-05
Backdoor.IRC.Aladinz.M	M	CyberNotes-2004-05
Backdoor.IRC.Loonbot	N/A	CyberNotes-2004-05
Backdoor.IRC.MyPoo	**N/A**	**Current Issue**
Backdoor.IRC.MyPoo.Kit	**N/A**	**Current Issue**
Backdoor.IRC.Spybuzz	**N/A**	**Current Issue**
Backdoor.Kaitex.E	E	CyberNotes-2004-05
Backdoor.OptixPro.13.C	13.C	CyberNotes-2004-04
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.R3C.B	**B**	**Current Issue**
Backdoor.Ranky.E	**E**	**Current Issue**
Backdoor.Sdbot.S	S	CyberNotes-2004-01
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tumag	**N/A**	**Current Issue**
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBH	N/A	CyberNotes-2004-01
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Download.Chamber	**N/A**	**Current Issue**
Download.Chamber.Kit	**N/A**	**Current Issue**
Download.SmallWeb	**N/A**	**Current Issue**
Download.SmallWeb.Kit	**N/A**	**Current Issue**
Downloader.Botten	N/A	CyberNotes-2004-05
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader-GD	GD	CyberNotes-2004-01
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpoof	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
Java.StartPage	N/A	CyberNotes-2004-05
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03
MultiDropper-GP.dr	GP.dr	CyberNotes-2004-04
MultiDropper-JW	**JW**	**Current Issue**
Needy.C	C	CyberNotes-2004-03
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
Phish-Potpor	N/A	CyberNotes-2004-04
Proxy-Agent	N/A	CyberNotes-2004-03

Trojan	Version	CyberNotes Issue #
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Bancos.E	E	CyberNotes-2004-05
PWSteal.Bancos.F	**F**	**Current Issue**
PWSteal.Bancos.G	**G**	**Current Issue**
PWSteal.Banpaes.C	C	CyberNotes-2004-05
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Irftp	N/A	CyberNotes-2004-05
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01
PWSteal.Tarno.B	B	CyberNotes-2004-05
PWSteal.Tarno.C	**C**	**Current Issue**
QReg-9	9	CyberNotes-2004-04
Spy-Peep	**N/A**	**Current Issue**
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/Badparty-A	**A**	**Current Issue**
Troj/Bdoor-CCK	CCK	CyberNotes-2004-05
Troj/BeastDo-M	M	CyberNotes-2004-01
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Cidra-D	D	CyberNotes-2004-05
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
Troj/DDosSmal-B	B	CyberNotes-2004-04
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Domwis-A	A	CyberNotes-2004-05
Troj/Eyeveg-C	C	CyberNotes-2004-05
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/HacDef-100	100	CyberNotes-2004-05
Troj/Hackarmy-A	A	CyberNotes-2004-02
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNot es-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey -A	A	CyberNotes-2004-02
Troj/Lalus-A	A	CyberNotes-2004-01
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/LDPinch-G	G	CyberNotes-2004-05
Troj/LDPinch-H	H	CyberNotes-2004-05
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linploit-A	A	CyberNotes-2004-02
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
Troj/Myss-C	C	CyberNotes-2004-04
Troj/Narhem-A	A	CyberNotes-2004-05
Troj/NoCheat-B	B	CyberNotes-2004-03
Troj/Noshare-K	K	CyberNotes-2004-02
Troj/Pinbol-A	A	CyberNotes-2004-04
Troj/Prorat-D	**D**	**Current Issue**
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Ranckbot-A	**A**	**Current Issue**
Troj/Ranck-K	K	CyberNotes-2004-05
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
Troj/Sdbot-FM	FM	CyberNotes-2004-04
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot -AA	AA	CyberNotes-2004-01
Troj/Spybot -AM	AM	CyberNotes-2004-01
Troj/Spybot -C	C	CyberNotes-2004-01
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Anymail	N/A	CyberNotes-2004-01
Trojan.Bansap	N/A	CyberNotes-2004-04
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Bookmarker.F	F	CyberNotes-2004-05
Trojan.Bookmarker.G	**G**	**Current Issue**
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Dustbunny	**N/A**	**Current Issue**
Trojan.Etsur	N/A	CyberNotes-2004-05
Trojan.Gema	N/A	CyberNotes-2004-01
Trojan.Gipma	N/A	CyberNotes-2004-05
Trojan.Gutta	N/A	CyberNotes-2004-04
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.KillAV.D	**D**	**Current Issue**
Trojan.Linst	**N/A**	**Current Issue**
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.Mitglieder.D	D	CyberNotes-2004-05
Trojan.Mitglieder.E	E	CyberNotes-2004-05
Trojan.Noupdate	N/A	CyberNotes-2004-05
Trojan.Noupdate.B	**B**	**Current Issue**
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
Trojan.PWS.QQPass.F	F	CyberNotes-2004-04
Trojan.Regsys	**N/A**	**Current Issue**
Trojan.Simcss.B	B	CyberNotes-2004-05
Trojan.Tilser	N/A	CyberNotes-2004-05
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
VBS.Bootconf.B	B	CyberNotes-2004-04
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
W32.Kifer	N/A	CyberNotes-2004-04
W32.Kifer.B	B	CyberNotes-2004-04
W32.Tuoba.Trojan	**N/A**	**Current Issue**
Xombe	N/A	CyberNotes-2004-01

Backdoor.Cazno.Kit: This is a Trojan editor or client that allows a malicious user to control systems that Backdoor.Cazno compromises.

Backdoor.Cazno: This is a Trojan horse that allows a malicious user to control a compromised system.

Backdoor.Danton: This Trojan allows unauthorized remote access. By default, the backdoor listens on port 6969.

Backdoor.IRC.MyPoo.Kit: This is a Trojan editor that allows a malicious user to create Backdoor Trojan horses. The Trojans created with this kit are detected as Backdoor.IRC.MyPoo**.**

Backdoor.IRC.MyPoo: This is a IRC backdoor Trojan. It is created using a Trojan editor, which is detected as Backdoor.IRC.MyPoo.Kit.

Backdoor.IRC.Spybuzz: This is a backdoor Trojan horse that uses Internet Relay Chat networks as its backdoor channels.

Backdoor.R3C.B: This is a Trojan horse that allows unauthorized access to an infected computer. By default, it opens port 9870 to listen for a connection. The Trojan is written in the Delphi programming language.

Backdoor.Ranky.E: This is a Trojan horse that runs as a proxy server. By default, the Trojan opens TCP port 42321. It is written in Microsoft Visual C++ and is packed with FSG. When Backdoor.Ranky.E is executed, it opens TCP port 42321, so that it can receive commands from a malicious user. It runs as a proxy server on a compromised computer and adds the value, “Windows NNT" = "<path to trojan>,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

Backdoor.Tumag: This Trojan allows unauthorized remote access to an infected computer. By default, the backdoor listens on TCP port 9010.

Download.Chamber.Kit: This is a kit that allows a malicious user to create a downloader. The file that it creates is detected as Download.Chamber.

Download.Chamber: This is a downloader that is written in Visual Basic.

Download.SmallWeb.Kit: This is a Trojan creation kit. The Trojan's that are created with it can be configured to download and execute malicious files. The created Trojan is detected as Download.SmallWeb.

Download.SmallWeb: This is a Trojan horse that downloads executable, potentially malicious files, and then executes them. A Trojan editor's kit creates the Trojan. The kit is detected as Download.SmallWeb.Kit.

MultiDropper-JW: This Trojan is intended to drop malware onto the victim machine. The threat consists of multiple components: A HTML file containing an encoded VBS script. This HTML file is known to have been spammed out to users as an e-mail attachment:

- EXCHANGERS.ZIP (10,209 bytes), containing:
- EXCHANGERS.HTM (18,364 bytes)

The VBS within the HTML file is detected as VBS/MultiDropper-JW.gen with the specified engine/DATs. The script drops (and executes) an EXE file on the victim machine:

- NOTEPAD.EXE (7,168 bytes)

This EXE is detected as MultiDropper-JW with the specified engine/DATs. When run, this EXE drops another EXE:

- %WinDir%\USERINIT.EXE (14,336 bytes)

This EXE is also detected as MultiDropper-JW with the specified engine/DATs. When run, it drops another Trojan onto the victim machine:

- %WinDir%\CSRSS.EXE (11,264 bytes)

The following Registry key is modified in order to drop/execute the Trojan CSRSS.EXE upon system reboot:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon "userinit"

is changed from “%SysDir%\USERINIT.EXE,” to “%WinDir%\USERINIT.EXE. Additionally, the StartPage-CG Trojan alters the security settings of Internet Explorer. Values within the following key are altered:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

The following are all set to equal 0x00000000: "1001," "1004," "1200," "1201," "1405," and "1406."

PWSteal.Bancos.F: This is a Trojan horse that mimics the online interfaces of certain Brazilian banks to try to steal account information. It is a minor variant of PWSteal.Bancos.E.

PWSteal.Bancos.G: This is a Trojan horse that mimics the online interfaces of certain Brazilian banks to try to steal account information.

PWSteal.Tarno.C: This is a Trojan horse that attempts to intercept user names and passwords, and other computer information. It sends the user names and passwords to a certain e-mail address using its own SMTP engine.

Spy-Peep: This Trojan arrives in a dropper file. When the dropper is run, it creates the following two files in the Windows system (%SysDir) directory:

- service.exe (164,372)
- explorer.exe (81,920)

The following registry keys are created:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon "Shell" = %SysDir%\explorer.exe
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventNotification "DisplayName" = COM+ Event Notification
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventNotification "ImagePath" = %SysDir%\service.exe –service

The Trojan attempts to download remote configuration file:

- Peep@203.202.128.50:443$$$

It can perform various operations according to the configuration, such as:

- Gather and send machine specific information
- Download and execute file
- Open socket and send data to other hosts

Troj/Badparty-A: This Trojan displays a message box containing the text 'Press OK to install the party invitation....' When the user clicks on OK the Trojan deletes the partition table in the master boot sector and the contents of the FAT. The Trojan then attempts to create a new partition table. The Trojan creates the following files, which are all copies of legitimate utilities: ginst0.dll in the Windows temp folder, int86_16.dll, int86_32.dll, playme.exe, and party.ini in the Windows folder.

Troj/Prorat-D: (Alias: Backdoor.Prorat.15): This is a backdoor Trojan which may allow unauthorized access and control of the computer from a remote network location. Upon execution, Troj/Prorat-D drops copies of itself into the Windows System or System32 folder using one or more of the filenames FSERVICE.EXE, FFSERVICE.EXE, DSERVICE.EXE, LSERVICE.EXE, SSERVICE.EXE, and WSERVICE.EXE. Troj/Prorat-D adds the following registry entries so that it is run on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Reg Services = C:\<Windows System>\<filename>
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Reg Services = C:\<Windows System>\<filename>
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell = Explorer.exe C:\<Windows System>\<filename>
- HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\Windows Reg Services = C:\<Windows System>\<filename>
- DirectX for Microsoft Windows = C:\<Windows System>\<filename>
- HKLM\Software\Microsoft\Active Setup\Installed Components\[A75aed00-d7bf-11d1-9947-00c0Cf98bbc9]\StubPath = C:\<Windows System>\<filename>
- HKLM\Software\Microsoft\Active Setup\Installed Components\[5Y99AE78-58TT-11dW-BE53-Y67078979Y]\StubPath = C:\<Windows System>\<filename>

This Trojan may also attempt to download and install the file ttp://members.lycos.co.uk/kabloboy/XP_Update v1.5.3.exe. This will be copied into the Windows folder under WINLOGON.EXE. This program will drop the file WINKEY.DLL into the Windows System folder and create the following registry entry:

- HKCU\Software\Microsoft DirectX\WinSettings\

Troj/Prorat-C is embedded within WINKEY.DLL. The downloaded file will also change the value in the [boot] and [windows] sections of the files SYSTEM.INI and WIN.INI (respectively), in the Windows folder by including the path to a copy of the original file. Troj/Prorat-D may also employ counter-removal tricks so that it becomes difficult to terminate the Trojan process. Furthermore the Trojan may monitor the registry entries above such that the entries are restored immediately if changed.

Troj/Ranckbot-A (Aliases: TrojanProxy.Win32.Ranky.p, Backdoor.SdBot.ev, W32/Sdbot.worm.gen.b, Proxy-FBSR.gen): This Trojan drops the files fqvwot.exe and wcs.exe into the folder WinNT\system32 and runs them. These files are detected as W32/Sdbot-EV and Troj/Ranck-M. W32/Sdbot-EV copies itself to the file svchosts11.exe in the Windows system folder and creates the following registry entry, pointing to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsong

Troj/Ranck-M creates the following registry entry to start itself automatically when Windows boots up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows NT

Trojan.Bookmarker.G: This Trojan modifies the Internet Explorer settings, adds bookmarks to Internet Explorer Favorites, and downloads other programs.

Trojan.Dustbunny: This Trojan displays this message: “Bad Pirate! So, you think you can steal from software companies do you? That's called theft, don't worry your secret is safe with me. Go thou and sin no more.” Then, it sends a notification message to a Web server for logging purposes. This program was recently distributed with deceptive file names on peer-to-peer file-sharing networks. Its purpose appears to be to track software piracy and illegal file sharing.

Trojan.KillAV.D: This is a Trojan horse that attempts to terminate many antivirus products on an infected system. When Trojan.KillAV.D is executed, it copies itself as %Windir%\<Trojan file name> and adds the value, “<Trojan file name> = %Windir%\<Trojan file name>,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It also adds the value, “load"=%Windir%\<Trojan file name>,” to the registry key:

- HKEY_Current_User\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

Trojan.Linst: This Trojan attaches itself to Internet Explorer and sends information to a Web server.

Trojan.Noupdate.B: This is a Trojan horse that attempts to prevent users from updating their computer with the latest Microsoft Windows patches and antivirus updates.

Trojan.Regsys: This Trojan modifies registry settings and delete files from an infected system.

W32.Tuoba.Trojan: This Trojan uses an Internet Explorer exploit to add a Web server to the Intranet zone and to redirect network traffic to that server.